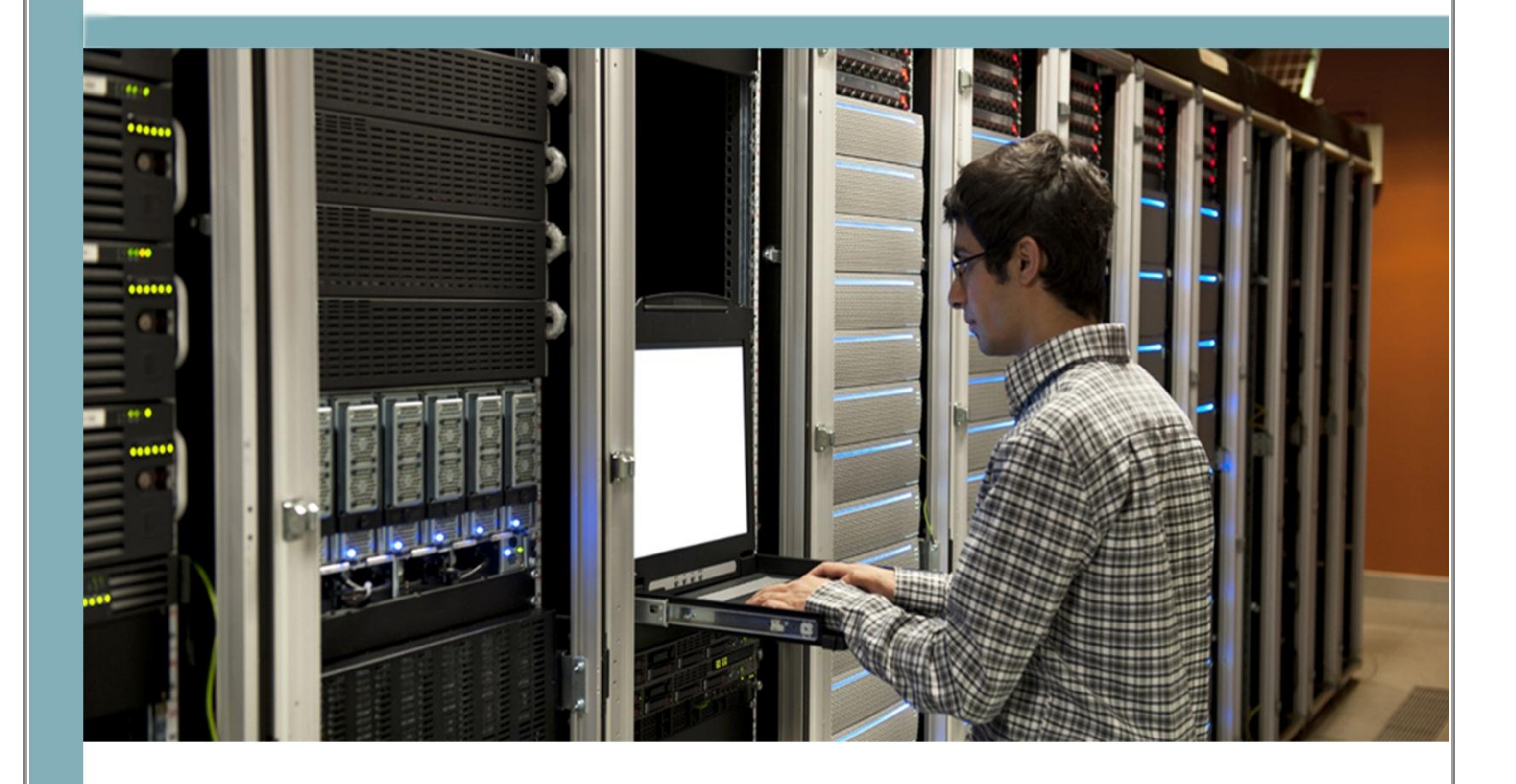
CISCO



CCNA R&S / Arabic

Level 1 , 2 , 3 , 4 , 5 , 6

Exam 200 - 125

By . Eng Ahmad H Mashaikh

بسم الله الرحمن الرحيم

هذا الكتاب إهداء إلى جميع العرب في كل العالم .

هدف الكتاب أن يسهل على كل من يريد الدخول إلى تخصص عالم الشبكات .

هذا الكتاب الذي أخذ مني الكثير من الوقت والمجهود ، ولا أريد مقابل من هذا الكتاب وكل ما أريده أن يستفيد منه جميع الناس.

أشكر كل من ساهم في عمل هذا الكتاب وبارك الله فيكم أخواني

المهندس وليد فتحى ، كل الشكر والتقدير لك أخي وليد على مجهودك في إشرافك على عمل الكتاب بشكل ممتاز بارك الله .

المهندس مهند هدهود ، كل الشكر و التقدير لك أخي مهند على مجهودك الرائع في مراجعة الكتاب .

المهندسة زينب اعبيدو ، كل الشكر والتقدير لكي على مجهودك الرائع في تدقيق الكتاب .

الكتاب من إعداد المهندس : أحمد حسن المشايخ

مختص أمن معلومات ونظم تشغيل وشبكات ، أعمل على نفسي بشكل كبير و مستمر على تطوير نفسي والوصول إلى درجة مستشار في شركة جوجل وسأستمر يوماً تلو الآخر في محاولة الوصول لهذا المستوى العظيم ، و من يعلم فربما يأتي يوماً وأكون مستشار من أحد مستشارين شركة جوجل العملاقة .

المعلومات الخاصة

الجنسية فلسطيني , مقيم في فلسطين

أعمل مدرب شبكات ونظم تشغيل وأمن معلومات .

المعلومات للتواصل والاستشارة أو المساعدة في أي مجال

E-Mail ahmad.private.mashaikh@gmail.com

Facebook : Ahmad H Mashaikh

Mobile: 00972598053163

المقدمة

يسأل الكثيرون عن شهادة سيسكو المعتمدة في الشبكات **Cisco Certified Network Associate** ما هي أهميتها كيفية الحصول عليها ومدتها و سنحاول باختصار أن نغطي الجزء الأكبر من التساؤلات.

CCNA هو منهج مُصمم لمدراء ومهندسو الشبكات يحتوي أساسيات للتخفيف من اختراق الشبكات ، مقدمة إلى الشبكات اللاسلكية : مفاهيم ومصطلحات، والمهارات الرئيسية في الشبكات كذلك يشمل على البروتوكولات **IP EIGRP, VLANs, Ethernet, :** و **ACLs** وغيرها.

ثم يقدم امتحان مباشر من الشركة (**On Line**) لإثبات قدرة المرشح على تثبيت وتشغيل واستكشاف الأخطاء في الشبكات وحلها مهما بلغت درجة التعقيد، ويمكنه تحويل وتوجيه الشبكات متوسطة الحجم حيث يتضمن مقدرته على تكوين عناوين **IP** وتعريفها بالإضافة لإنشاء اتصالات لمقدمي الخدمات من خلال شبكات واسعة المدى (**WAN**) .

وتثبت أن المرشح متمكن من منتجات سيسكو المختلفة وأنه على معرفة واسعة بتقنيات الشبكات وبروتوكولاتها.

يمكن أن يتخذ هذا الامتحان أحد الشكلين التاليين:

الأول: أن يُؤخذ **CCNA** في امتحان واحد يطلق عليه **CCNA 200-120 , 200-125**

الثاني: أن يُؤدى في امتحان من جزئين يطلق عليها (**ICND1 and ICND2**) اختصاراً لـ **Interconnecting Cisco Network Devices 1 and 2**

يشمل الامتحان المواضيع الرئيسية والمبادئ التوجيهية لمحتوى **CCNA 200-120:** امتحان **CCNA** المُركب :

شرح لكيفية عمل الشبكة

تكوين الشبكة والتحقق منها واستكشاف الأخطاء وحلها.

تنفيذ خطة لمعالجة عناوين **IPs** و خدمات **IP** للاشتراك في الشبكة.

اختيار وشرح المهام الإدارية اللازمة لـ **WLAN**

تعريف التهديدات الأمنية على الشبكة وتوصيف الطرق المثلى لمواجهه هذه التهديدات.

تنفيذ و مراقبة روابط الشبكات واسعة المدى.

مما لا نغفل عن ذكره أن الشهادة صالحة للاستخدام لمده ثلاث سنوات منذ الحصول عليها، يمكن الحاصل عليها بعد ذلك أن يدخل الامتحان مرة أخرى أو ينتقل لشهادات أكبر مثل **CCNP** أو **CCDP**.

فهرس المستوى الأول

Networking Fundamentals أساسيات الشبكات

تاريخ تطور شبكات الحاسوب

تاريخ تطور الشبكات :

تطوّر الإنترنت نتيجة أبحاث بدأت في أوائل الستينيات حين عزمت وزارة الدفاع الأمريكية دخول مشروع ربط الحواسيب الرئيسية حينئذٍ والتابعة لوزارة الدفاع بالاتصال بعضها مع بعض؛ وذلك لتشكيل شبكة ذات عدة مراكز. أي أنها شبكة تصلح نفسها بنفسها، والشبكة التي صممت عرفت باسم **ARPANET Advanced Research Project Agency Net** . في فترة الثمانينيات أخذت مؤسسة العلوم الوطنية (**NSF**) الأمريكية **National Science Foundation** برنامجًا موسعًا لربط الحواسيب المركزية العملاقة مع **ARPANET** ، وبدأت الجامعات ومراكز الأبحاث الآخر في العالم الانضمام لهذه الشبكة وفي١٩٩١ نشأت شبكة الويب العالمية (**www**)قام تيم بيرنرز لي بتطوير كود (**www**) شبكة الويب العالمية (**World Wide Web**) ثم في **١٩٩٣** تم وضع ميثاق مجتمع الإنترنت (**ISOC**) ، تجاوز عدد مضيفي (مستخدمي) الإنترنت ١.٠٠٠.٠٠٠وفي ١٩٩٤ ظهور برنامج **Netscape Navigator. 1996**تجاوز عدد مضيفي (مستخدمي) الإنترنت عشرة ملايين، غطت شبكة الإنترنت الكرة الأرضية.من أواخر التسعينيات من القرن العشرين وحتى الآن يتضاعف عدد مستخدمي الإنترنت كل ستة أشهر تجاوز عدد مضيفي (مستخدمي) الإنترنت ١١٠ مليون.في ٢٠٠١ السمات الخاصة بالشبكة: لعمل شبكة حاسوب يجب توافر المتطلبات التالية: وسيط ناقل عبارة عن أسلاك أو وسائط لاسلكية. مؤائم لتوصيل تلك الوسائط إلى الشبكة .

شبكات الحاسوب :

شبكة الحاسوب هي نظام لربط جهازين أو أكثر باستخدام إحدى تقنيات نظم الاتصالات من أجل تبادل المعلومات والموارد والبيانات بينها المتاحة للشبكة مثل الآلة الطابعة أو البرامج التطبيقية أياً كان نوعها وكذلك تسمح بالتواصل المباشر بين المستخدمين. وبشكل عام تعتبر دراسة شبكات الحاسوب أحد فروع علم الاتصالات. من الممكن أن تكون أجهزة الحاسوب في الشبكة قريبة جداً من بعضها وذلك مثل أن تكون في غرفة واحدة وتسمى الشبكة في هذه الحالة شبكة محلية **LAN** ومن الممكن أن تكون الشبكة مكونة من مجموعة أجهزة في أماكن بعيدة مثل الشبكات بين المدن أو الدول وحتى القارات ويتم وصل مثل هذه الشبكات في كثير من الأحيان بالانترنت أو بالسواتل (**Satellite**) و تسمى الشبكة عندها شبكة عريضة **WAN** ، هناك أيضاً في مقابل ذلك الشبكة الشخصية **PAN** والتي تربط مجموعة أجهزة قريبة من المستخدم.

تقسيم الشبكات : تقسم الشبكات إلى عدة أقسام حسب مدى الشبكة إلى : شبكة عريضة أو الشبكات الواسعة شبكات تستخدم للمسافات البعيدة مثل الانترنت الشبكات المحلية تستخدم لمسافات أقرب مثل الشبكات التي تستخدم في الجامعات **Local Area Network LAN** يغطي هذا النوع من الشبكات عادة المناطق الجغرافية الصغيرة مثل الجامعات أو أحد فروع الشركات الكبيرة أو شبكة الحاسوب في منزل ما. عدد أجهزة الحاسوب في هذا النوع يتراوح على الأقل من جهازين إلى **500** ولربط هذه الأجهزة نحتاج إلى جهاز يسمى الهب**hub** أو المبدل **switch** أي المركز أو الناقل ليعمل على ربط الأجهزة معا ويمكنها من الاتصال ببعضها البعض. يستخدم لربط الأجهزة عادة في مثل هذا النوع من الشبكات أسلاك وهي من نوع خاص لنقل البيانات أو الأجهزة اللاسلكية.يتمكن المتصل في الشبكة من رؤية المعلومات والملفات الموجودة على أجهزة الآخر ين إن سمح له بذلك.يستخدم هذا النوع عادة في المؤسسات الصغيرة والجامعات من أجل تسهيل العمل ونقل المعلومات المشتركة بين الأقسام بشكل سريع.

تتوافر عدة طرق للوصل بين الشبكة الحاسوبية، منها:

١. طريقة الوصل المختلطة Mesh networks .
٢. طريقة الوصل النجمية Star networks.
٣. طريقة الوصل الخطية Bus networks.
٤. طريقة الوصل الشجرية Tree networks.
٥. طريقة الوصل الحلقية Ring Topology.

وسيتم شرح كل من هذه الأنواع بالتفصيل.

أهداف و فوائد الشبكات :

ظهرت الشبكات نظراً للحاجة إلى الاتصال بين الأفراد في الأماكن المتباعدة وتبادل الخدمات المختلفة، وساعد في ذلك التطور العلمي والتقني . لذلك دعت الحاجة إلى إِنشاء نظام يمكن للمستخدم المشاركة في مصادر المعلومات مثل ربط فروع الشركة المنتشرة في عدة مناطق بنظام واحد و كذلك المشاركة في الأجهزة و البرامج مثل ربط آلّة الطباعة بعدة أجهزة بدلا من أن يكون لكل جهاز طابعة خاصة. لذلك فان الشبكات سوف توفر بيئة عمل مشتركة و التي سوف تمكن المسؤولون في الشركة من الادارة والدعم المركزي على مستوى جميع فروع الشركة أو المؤسسة المنتشرة في عدة مناطق جغرافية. لذلك نجد أن هنالك عدة

أسباب دعت و أدت إلى انشاء شبكات الكمبيوتر ومن أهم هذه الأسباب التالي :

١ - المشاركة في البرامج و البيانات.
٢ - المشاركة في موارد الشبكة .
٣ - الدخول على انظمة تشغيل تكون متباعدة المسافة .
٤ - دعم الادارة المركزية للنظام .
٥ - امكانية انشاء مجموعات عمل موحدة على مستوى مناطق جغرافية متباعدة .

و مع هذه الأسباب التي أدت إلى انشاء شبكات الحاسب هنالك عدة فوائد من ربط الأجهزة في شبكة واحدة، وقبل الشروع في هذه الفوائد سنأخذ هذا السيناريو والذي سيثبت لنا مدى الفائدة انشاء تلك الشبكات السيناريو لنتخيل وضع شركة ما لها عدة فروع في عدة مناطق لكن بدون شبكة تربط بين فروعها، في هذه الحالة كيف سوف يتم استبدال البيانات. سنحتاج إلى مئات الأقراص المرنة و مئات أجهزة التخزين لنقل المعلومات من جهاز إلى آخر ومن فرع لآخر و هذا سيؤدي إلى هدر كبير من الوقت والجهد. و اضف إلى ذلك أنه بدون شبكة سنحتاج إلى طابعة واحدة لكل جهاز وهذا يسبب عبء وهدر كبير في موارد المؤسسة.

من خلال السيناريو السابق نستنتج أهمية وجود تقنية الشبكات والتي تتلخص في التالي :

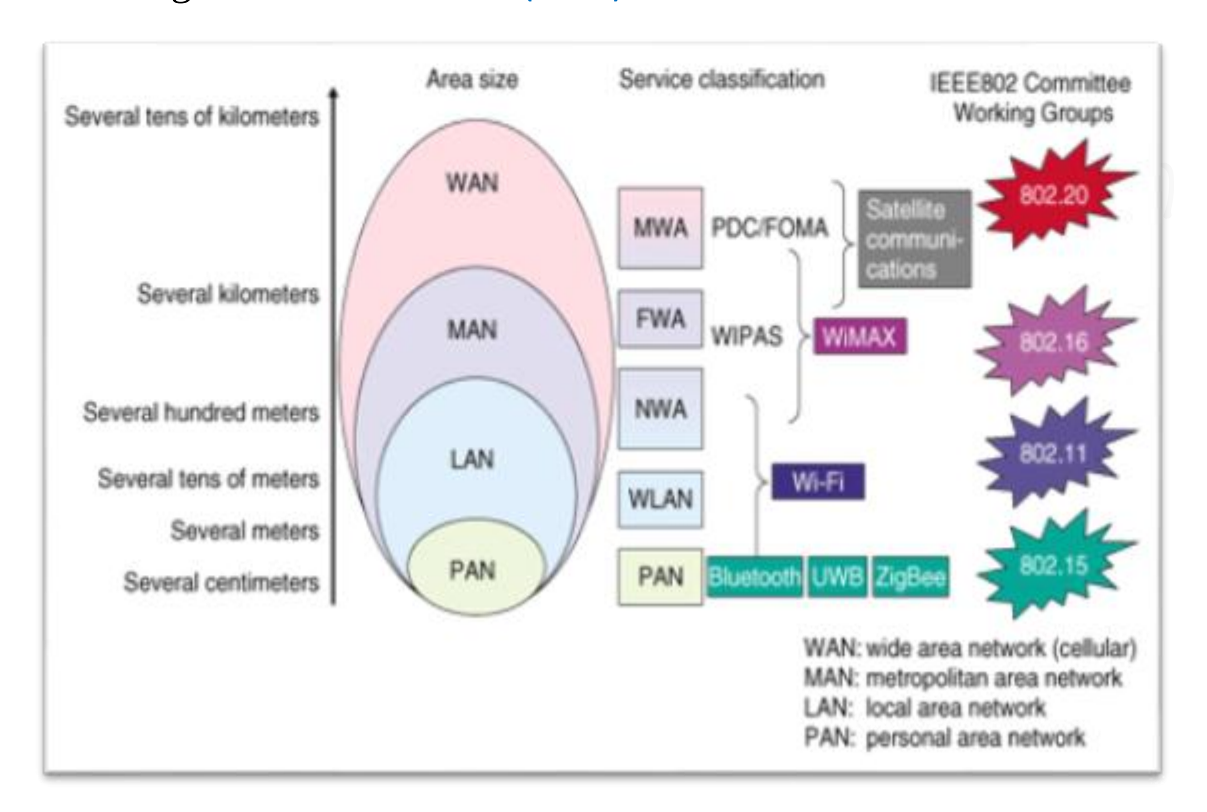
١ - توفير المال و الذي يسهم في تخفيض و تقليص التكاليف الأقتصادية عبر ما تقدمه الشبكة من خدمات تعجز الحواسيب المفردة من تقديمها .
٢ - توفير الوقت والجهد في نقل البيانات من مكان لآخر .
٣ - تسمح تقنية الشبكات من ادارة المؤسسة بشكل مركزي حيث يمكن لكل مستخدمي الشبكة استخدام نفس البيانات في نفس الوقت مع اختلاف المناطق الجغرافية .
٤- امكانية التوسع على مستوى النطاق الجغرافي مع أقل تكلفة مبذوله مما يؤدي إلى زيادة الإنتاجية.



أنواع الشبكات من حيث المدى الجغرافي

Types of Networks by Geographical Area

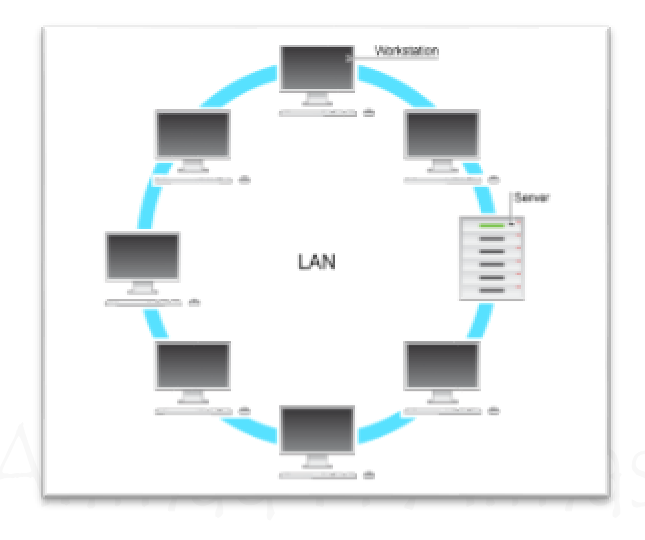
Local Area Networks - (LAN)	شبكة المناطق المحليه
Wide Area Networks - (WAN)	شبكة المناطق الواسعه
Campus Area Networks - (CAN)	شبكة المباني
Personal Area Networks - (PAN)	شبكة خاصة
Metropolitan Area Networks - (MAN)	شبكة المدينة
Wireless Local Area Networks - (WLAN)	الشبكة اللاسلكي
Global Area Networks - (GAN)	الشبكة العالمية
Storage Area Networks - (SAN)	الشبكة التخزينية



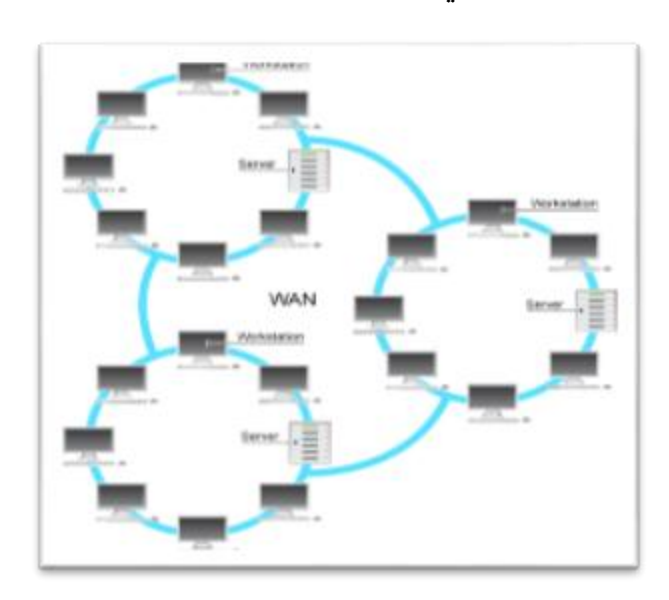
البنية التحتية للشبكة : تتمثل في المكونات المادية وهذه المكونات تتكون في داخل الشبكة وتجعل الأجهزة قادرة على الاتصال ببعضها البعض وتتبادل البيانات فيما بينهما تتمثل هذه المكونات في الكيابل و نقاط الشبكة أجهزة الشبكة مثل الراوترات و السويتش ات و السيرفرات و الكثير من هذه الأجهزة سنقوم بشرح هذه الأجهزة في الدروس القادمة .

- الآن سأقوم بشرح كل من هذه الأنواع بالتفصيل مع امثله على كل نوع من هذه الشبكات :

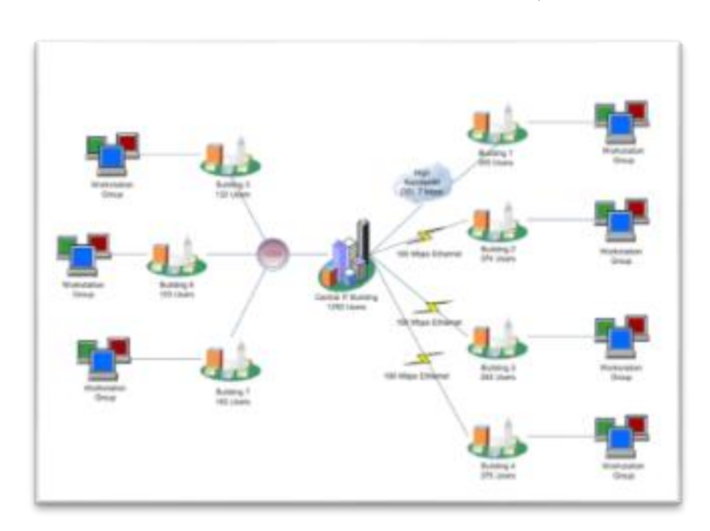
LAN : هذه الشبكة المحلية محدودة المساحة و هي عبارة عن شبكة تربط بين عدة حاسبات ولكن داخل منطقة جغرافية صغيرة مثل مبنى مكون من اكثر من طابق أوعدة مباني مجاورة أو مثل جامعة أو مستشفى أو شركة وهي من أكثر الشبكات أنتشاراً، هذه الشبكة كل ما يتكون منه من معدة أو برامج أو حاسبات هي ملك للشركة، سنقوم بعمل شبكة حقيقة لهذه الشبكة في الدروس القادمة و كيفية العمل فيها و التحكم فيها.



WAN : هذه الشبكة الواسعة مفتوحة المدى وهي من أكثر الشبكات انتشاراً وهي غير محدودة من ناحية المساحة الجغرافية و وظيفة هذه الشبكة إنه تقوم بربط الدول و المدن البعيدة في بعضها البعض وايضاً تقوم بربط الشبكات المحلية ببعض و ربط فروع الشركة في بعض ايضاً هذه الشبكة من أكبر الشبكة الموجوده في العالم سنقوم بشرح بعض أجزاء هذه الشبكة في الدروس القادمة.



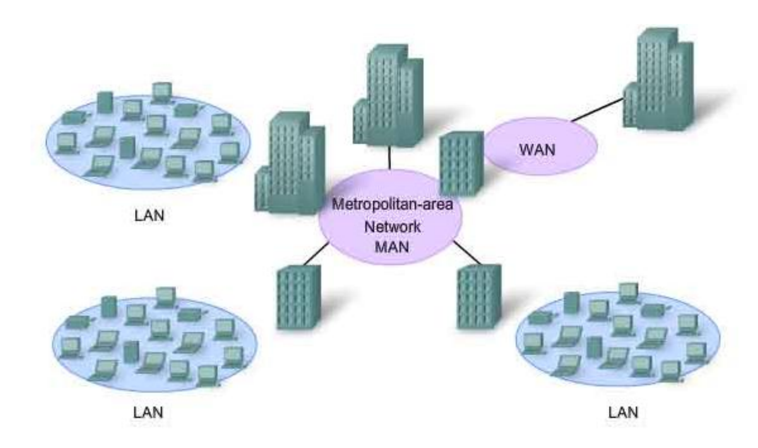
CAN : هذه الشبكة من حيث المدى تعتبر الشبكة الوسيطة ما بين الشبكة المحلية و الشبكة الواسعة المحدودة فهذه الشبكة تستخدم في المنازل و المكاتب و المقاهي هذا النوع من الشبكات لا يستخدم كثيراً ولكن يجب ذكره للمعرفه.



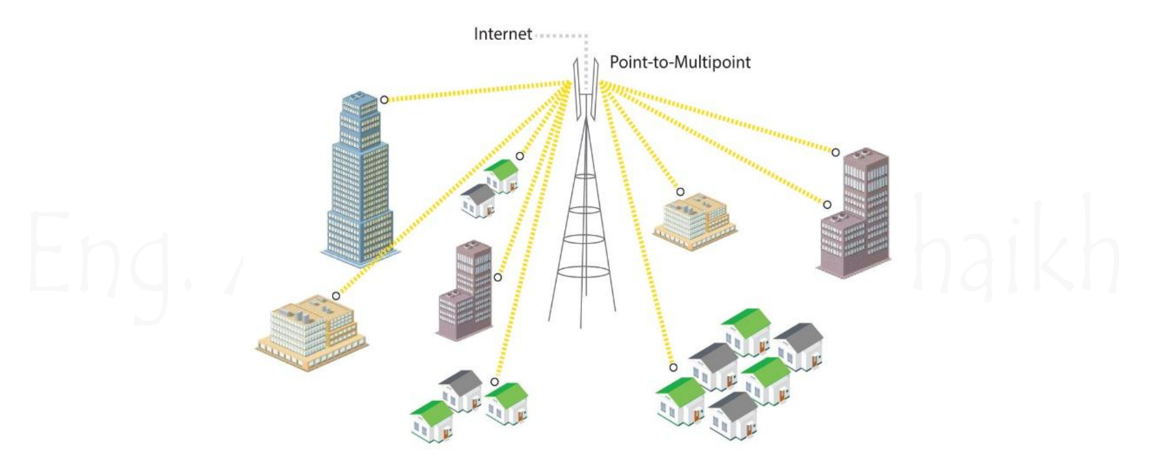
PAN : هذه الشبكة من النوع الخاص مسافتها لا تتعدى الـ ١٠ أمتار وتستخدم أحياناً للوصول بين جهازين كمبيوتر أو فاكس أو طابعة و تستخدم في أغلب الأحيان تقنية البلوتوث اي أن الاتصال يتم بشكل لا سلكي بأستخدام موجات لا سلكية.



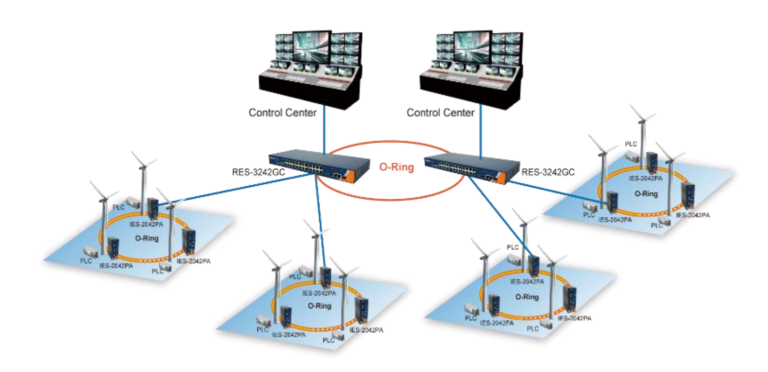
MAN : هذه الأنواع من الشبكات تصل بقعتها الجغرافية لتظم مدينة كاملة أو عدة مدن و من امثلتها القنوات التلفزيونية التي تبث في مدينة معينة أو عدة مدن متقاربة وكذلك بعض المؤسسات المتوسطة الحجم والتي قد تنتشر في المدينة هنا وهناك يعني مثلا بعض دوائر الدولة من بلدية وبيئة والتي تتصل جميعها بمركز المحافظة أو الاقليم و عادة ما تتكون شبكة الـ (**MAN**) من عدة شبكات (**LAN**) متصلة فيما بعضها.



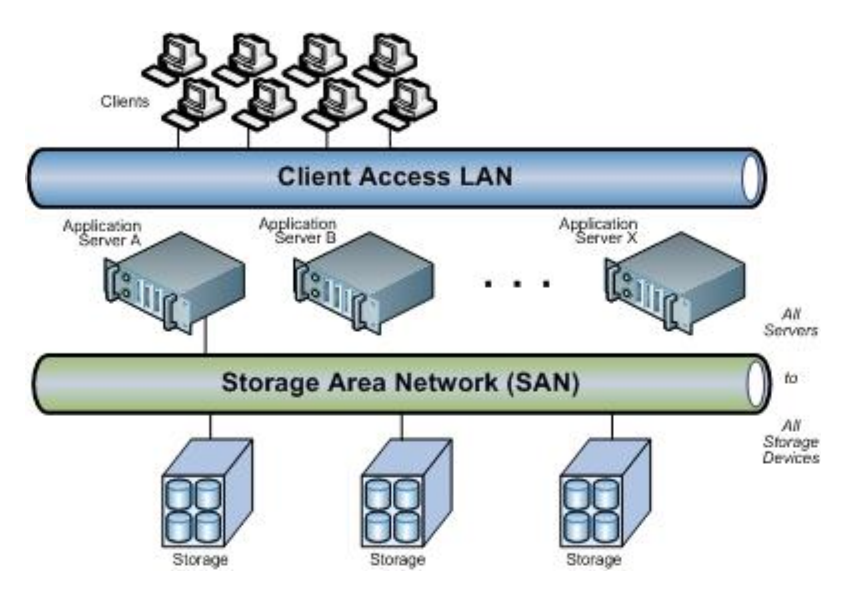
WLAN : الشبكة اللاسلكية هذه من الشبكة التي تستخدم موجات الراديو للاتصال بين بعضها البعض ولها ترددات خاصة وهذه الشبكة له كورسات خاصة يتم دراسة هذا الكورس لتتكمن من التعامل مع هذه الشبكة بشكل صحيح و مفهوم وسنقوم بشرح بعض منه في الدروس القادمة.



GAN : هذه الشبكة تستخدم في العادة في شبكة الاتصالات لربط شبكات الموبايل و الهواتف الارضية ببعضها البعض لتتمكن من الاتصال ببعضها البعض.



SAN : هذه الشبكة تتصل في السيرفرات بشكل مباشر ليتم ايصال السيرفرات مع وحدة التخزين و مركز المعلومات الرئيسي و هذا النوع يستخدم تقنيات عالية السرعة مثل كوابل الفايبر وغيره سنقوم بشرح بعض التقنيات في الدروس القادمة.



معمارية الشبكة

Network Architectures

يوجد نوعان من معمارية الشبكات يتم بناء الشبكة على هذا الشكل التالي :

شبكة الند للند أو نقطة لـ نقطة Peer – to – Peer Networks

شبكة العميل و الخادم Client / Server Networks

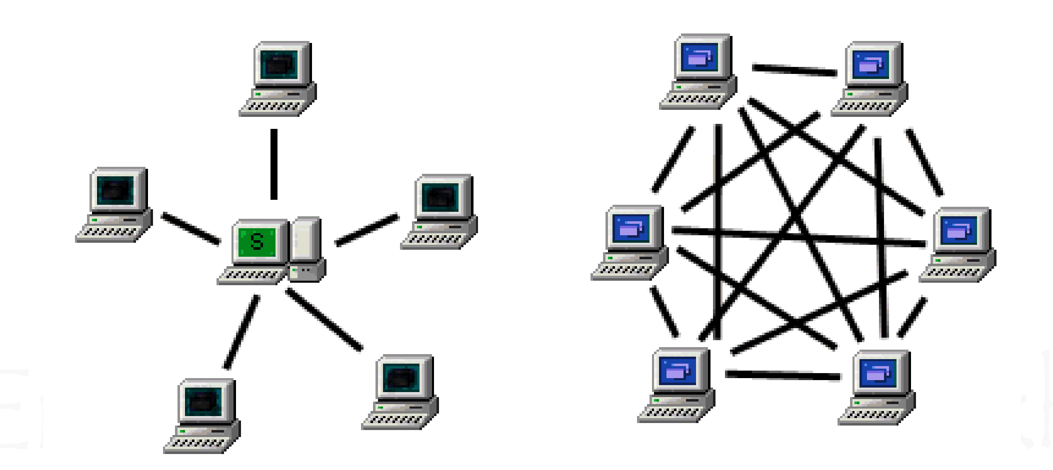
سأقوم بشرح كل منهم بالتفصيل و كل من مميزات هذه الشبكات لكل منهم مميزاته و عيوبه سأقوم بشرحهم بالتفصيل :

شبكة الند للند- Peer – to – Peer

١- تستطيع المشاركة في الملفات و الطابعة و الموديم .
٢- أي شخص يستطيع الاتصال في الشبكة .
٣- لا يوجد وحدة تحكم مركزية في الشبكة .
٤- كل مستخدم في الشبكة يقوم بتركيب البرامج الخاص فيه كم يريد .
٥- اتساع محدود للشبكة من ناحية عدد الأجهزة مثل اقصى عدد **20** جهاز كمبيوتر يطلق على هذه الشبكة **Workgroup**.
٦- لا يوجد وحدة تخزين موحده لكل مستخدم يكون له وحدة تخزين خاصة فيه.

- شبكة المضيف و الخادم Client / Server

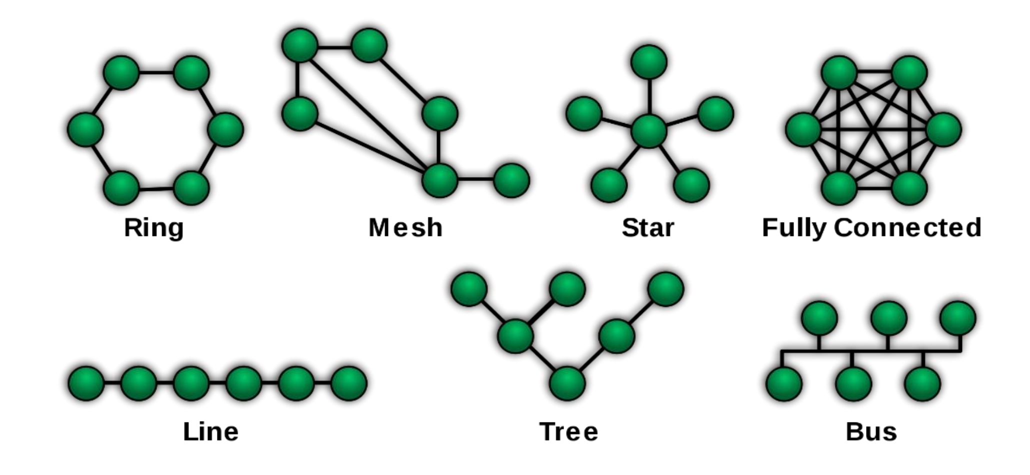
١- نستطيع المشاركة في كل الملفات و الطابعة و خطوط الانترنت .
٢- فقط الاشخاص المصرح لهم يستطيعون الدخول للشبكة .
٣- يوجد وحدة تحكم مركزية في الشبكة .
٤- عملية الصيانة أصعب .
٥- أتساع غير محدود من ناحية الأجهزة في الشبكة .
٦- نستطيع التحكم في كل أجهزة الشبكة من مكان واحد .



أنواع الشبكات حسب التصميم الهندسي

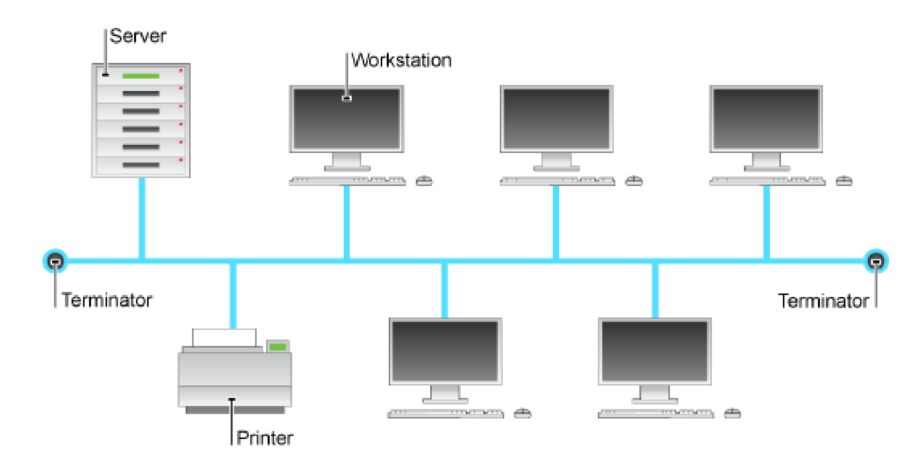
Physical Network Topologies

يوجد عدة تصاميم للشبكات من ناحية التصميم الهندسي على ارض الواقع و يوجد أكثر من نوع لهذه الشبكات سنقوم بشرح كل من هذه الشبكة بالتفصيل مع ذكر بعض الامثلة على كل شبكة .



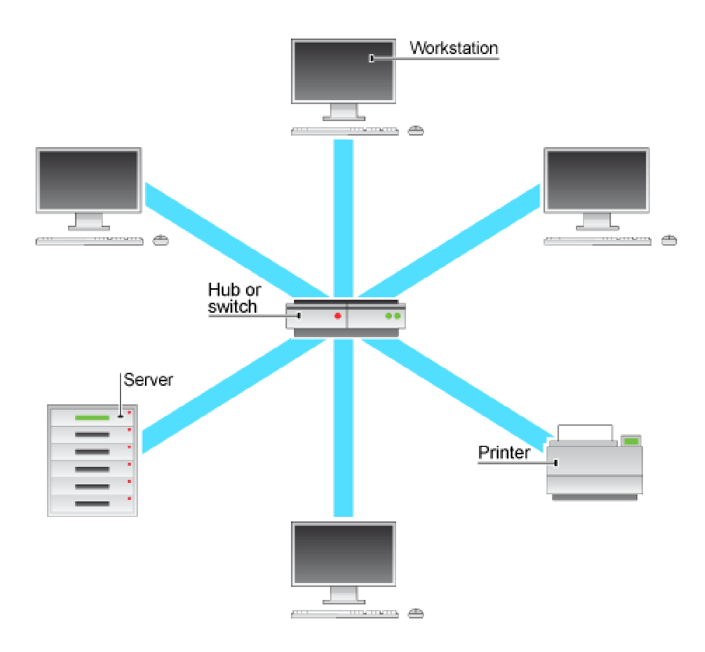
الشبكة الخطية Bus Topology :

هذه الشبكة لا توجد فيها وحدة تحكم مركزية و على ذالك فهي تتكون من كابل واحد يتصل فيه كل الشبكة و جميع الأجهزة و يتم نقل البيانات و المعلومات من جهاز لاخر عبر ما يسمى بالموصول أو الناقل وهي أدارة نقل بين جهازين أو أكثر ويتم ذالك في وضع نهاية الطريقة طرافية في نهاية الشبكة يسمى هذا الجهاز **Terminator** و الكابل الرئيسي الذي يربط جميع الأجهزة في الشبكة يسمى الـ **Backbone**.



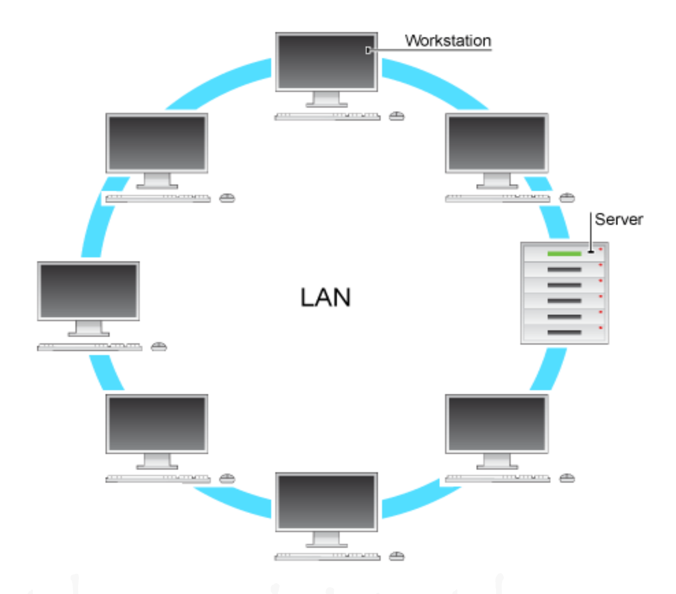
الشبكة النجمية Star Topology :

هذه الشبكة لا يوجد فيها كابل واحد رئيسي بل يوجد فيها أكثر من كابل مثل يوجد سوتيش و يتم ربط جميع الأجهزة على هذا السويتش ولكل جهاز كابل خاص وفي حال تعطل أحد الكوابل لا تتوقف الشبكة كله فقط يتم توقف الجهاز الذي تم توقف الكابل الخاص به هذه الشبكة أكثر أنتشاراً و شيوعاً في عالم الشبكة المحلية نظراً لسهولة الصيانة و العمل فيها ولها الكثير من المميزات العملية سيتم ذكرها في ما بعد .



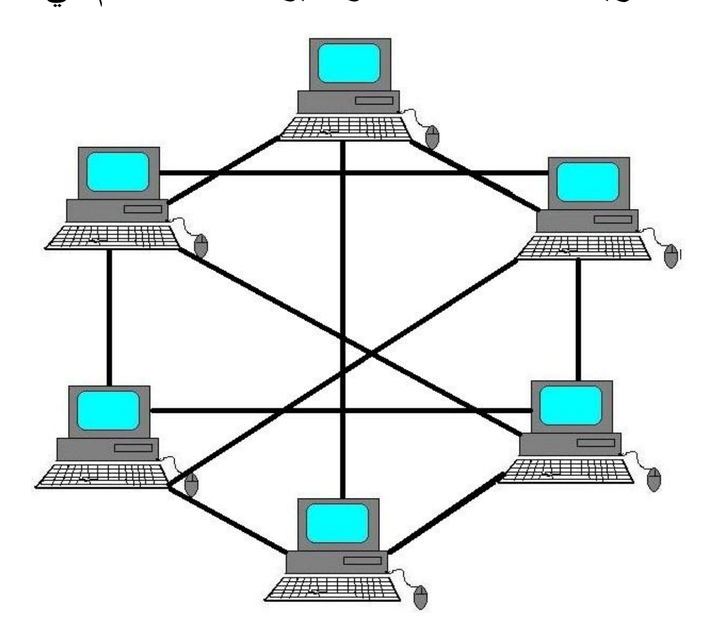
الشبكة الحلقية Ring Topology :

هذه الشبكة تستخدم كابل في كل جهازين وهي شبكة على شكل دائرة من الكابلات لربط مجموعة من الحاسبات معاً ويعتبر الحاسب المركزي جزء من الحلقة وتتحرك البيانات بشكل دائرة مما يتسبب في حدوث بطء في الشبكة و غيرها من المشاكل الآخر .



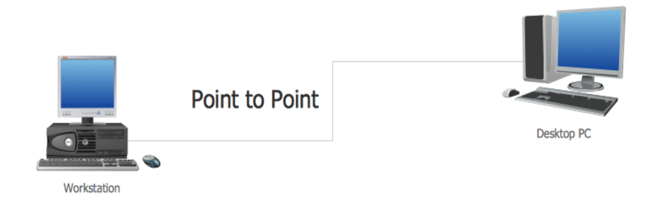
الشبكة المعقدة Mesh Topology :

هذه الشبكة تسمى المعقدة لإنه تحتوي على أكثر من كابل في كل جهاز و تحتوي على مجموعة من الكوابل المربوطة في كل الأجهزة و في جميع الأجهزة يخرج كابل على عدد الأجهزة الموجودة مثل لو كان لدينا خمسة أجهزة كمبيوتر سيتم أخذ من كل جهاز خمسة كوابل و الجهاز المقابل خمسة كوابل وهكذا حتى يتم الاتصال في جميع الأجهزة هذه الطريقة مكلفة جداً جداً ولا يوجد له أستخدام في الحياة العملية .



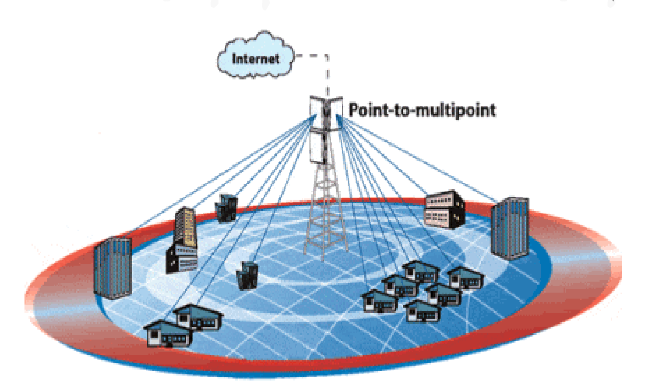
شبكة الند للند Point to point Topology :

هذه الشبكة تربط الأجهزة في بعضها البعض بشكل مباشر من غير تدخل أية جهاز للربط مثل جهاز كمبيوتر يتم ربطه بجهاز كمبيوتر أخرى بشكل مستقيم من غير أجهزة ربط مثل الراوتر يتم ربطه بشكل مستقيم مع راوتر أخرى مثل السويتش يتم ربطه بسوتيش أخرى بشكل مستقيم بمعنى أخى جهاز مقابل جهاز .

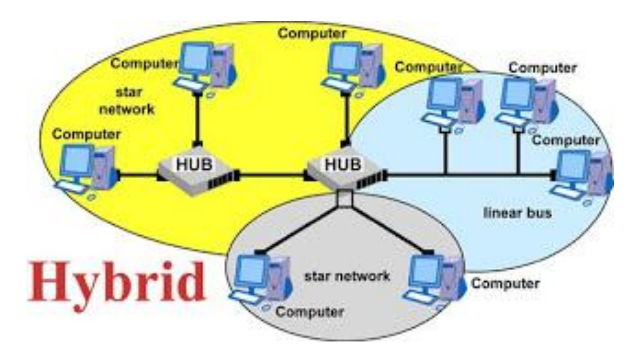


شبكة الإرسال و الاستقبال Point to Multipoint Topology :

هذه الشبكة تمثل الشبكة التي تستقبل و ترسل من مقسم رئيسي مثل يوجد سنترال يقوم بجمع جميع الأجهزة في مكان واحد ويتم الإرسال و الاستقبال من داخل السنتر مثل لو كان يوجد ثلاث شبكات كل شبكة في مبنى و نريد الشبكة أن تتبادل المعلومات و البيانات في ما بينهم سنقوم بربط المبنى الأول و الثاني في السنترال و عن طريق السنترال سيتم التحكم و الإرسال و الاستقبال .



شبكة الخليط **Hybrid Topology Network :** هذه الشبكة تسمى الهجين أو الخليط لأنه تربط ما بين شبكات مختلفة الأنواع .



Physical Media

أنواع الكابلات و الموصلات في الشبكات

- الكابل هو الوسيط الذي تنتقل من خلاله البيانات و المعلومات من حاسب إلى أخرى في الشبكة أو من شبكة إلى شبكة أخرى.

أنواع الكابلات في عالم الشبكة يوجد الكثير من الكابلات سنقوم بشرح ثلاث من هذه الأنواع المستخدم في الشبكات :

١. Coaxial Cable الكابل المحوري.
٢. Twisted Pair Cable الكابل المزدوج.
٣. Fiber Optic Cable الكابل الضوئي.



Coaxial Cable   Fiber Optic Cable   Twisted Pair Cable

- سأقوم بشرح كل من هذه الأنواع بالتفصيل و شرح كل من مميزات هذه الأنواع المختلفة :

١- **Coaxial Cable :** هو نوع من أنواع الكابلات النحاسية المستخدمة ويتكون من سلك نحاسي محاط بمجموعة أسلاك مجدولة ويفصل بينهما طبقة عازلة, الكابل المحوري يصنع خصيصا لنقل الإشارات ويستخدم كثيرا لتوصيل جهاز راديو أو جهاز تسجيل بجهاز آخر. كما يستخدم من قبل شركات الهاتف والاتصالات . فالإشارات ما هي إلا موجات ترددات عالية . تتصل الشبكة المعدنية الواقية بالأرضي فلا تؤثر شوشرة من الخارج على السلك المحوري . يكون الكبل المحوري بقطر ٥ - ١٥ مليمتر , ويستخدم أيضا لنقل البث التلفزيوني وفي أجهزة الفيديو .ويعم استخدامه أيضا في شبكات الراديو السلكية واللاسلكية .حيث أن أطوال قصيرة منه تستخدم لربط أجهزة ومعدات الاختبار مثل مولدات الإشارة . ويستخدم على نطاق واسع لربط شبكات الكمبيوتر في المنطقة المحلية . ولكن يتم في الوقت الحاضر استبداله بالأسلاك المحورية المجدولة والألياف الضوئية. ومن استخداماته في الأعمال التجارية وشبكة إيثرنت ، **Ethernet** كما يربط بين محطة الإرسال التلفزيوني أو الإرسال الراديو وبينهوائي الإرسال وهذا النوع يسمى خط إرسال ترددات الراديو أو خط قفصي ويكون عالي القدرة.

٢- **تاريخ الكبل المحوري** : نتيجة للحاجة الملحة في ذلك الوقت بسبب تغير الأوضاع الاقتصادية والعلمية كان لا بد من إيجاد وسيلة من التكنولوجيا آنذاك تسهل عملية الاتصال والتواصل فجاء الحل باختراع الكبل المحوري.حيث اخترع عام ١٩٢٩م واستخدم لأول مرة عام ١٩٤١م وبعد ذلك قامت **AT&T** بتشكيل فريقها الأول الذي اعتمد على هذه التقنية.ثم انتقل النظام عام ١٩٤٠م الذي اعتمد على الكبل المحوري وغيرها من العوامل الآخر إلى الأسلاك المجدولة والألياف الضوئية حيث أصبحت هي البدائل.

٣- **بنية الكابل المحوري** : هو كبل واحد يتكون من اثنين الموصلات من هما الموصل الداخلي والخارجي وهي تشترك في نفس المحور لهذا سميت بالكبل متحد المركز.الموصل الداخلي يعزله عازل كهربائي عن الموصل الخارجي ويغلفهما طبقة واقية عازلة هي الآخر فيسهل استخدامه واستعماله .الموصل الداخلي هو عادة سلك رفيع تنتقل فيه الإشارات المرسلة ، مثل كابل إنترنت أو كبل تليفون أو إلى مضخم صوت .الموصل الخارجي هو عادة يكون الدرع مصنوع من نوع مختلف من المواد ويحيط بالموصل الداخلي ويفصلها عن بعض طبقة عازلة . و يكون الدرع مؤلفا من إسلاك مضفرة.

الكابلات المحورية والنظم المرتبطة بهأو ليست مثالية وهناك بعض الإشارات تشع من الكابلات. الموصل الخارجي له وظائف كثيرة وهي كدرع للحد من اقتران الإشارة إلى الأسلاك فهو يحمي من الحقول الكهرومغناطيسية. هناك العديد من الأنواع المختلفة من الكبل المحوري.لأن كل نوع منها مع الخصائص الفيزيائية والإلكترونية مختلف عن الآخر حيث أنه يصمم لأداء مهام معينة .

٤- **أستخدام الكابل المحوري** : الكابلات المحورية تصنع خصيصا لنقل الإشارات. لهذا تستخدبم في البث التلفزيوني والراديو وكذلك في وصلات الهاتف. تعمل لنقل الترددات العالية تحت جهد صغير.

تعمل لنقل عدد كبير من النطاق الترددي الذي يسمح لها لحمل إشارات متعددة مما يجعلها مثالية لاستخدامها في العديد من كابلات البث التلفزيوني. التدريع الواقي المتأرض يوفر حماية من التداخل الكهرومغناطيسي مما يسمح للإشارات على انخفاض القدرة على أن تنتقل لمسافات أطول وهو يمنع من اقتراب الإشارة إلى الأسلاك المجاورة مما يتيح زيادة أطوال الكبل الموصلة إلى مكبرات الصوت . الكبل المحوري يستخدم طوبولوجيا لربط شبكة الاتصال التي هي عرضة للاحتقان.

٥- **آلية عمل الكابل المحوري** : الطريقة التي يعمل بها الكابل المحوري هي طريقة بسيطة والإشارات التي تحتاج إلى أن تنتقل يتم إرسالها على طول الموصلات الداخلية والإشارة لا تتحرك في خط مستقيم لأن الانحناءات في الكبل المحوري تمنع ذلك من الحدوث ثم يأتي دور الموصل الخارجي فهو يتكون من الموصل المجدول الذي يوصل ويقي بذلك السلك المحوري الحامل للإشارات أي إشارة مشوشرة خارجية إلى الأرضي

الإشارة تفقد شيئا من طاقتها لأنها تسافر على طول الكابل . وهذه الخسارة في الطاقة تأتي في شكل فقدان الإشارة إلى الموصل الخارجي وهذا يجعل من فقدان إشارة الكبل المحوري أقل مثالية لتطبيقات كثيرة ولكن يمكن التغلب على ذلك في سكتها وتقوية الإشارات بواسطة مضخم إلكتروني

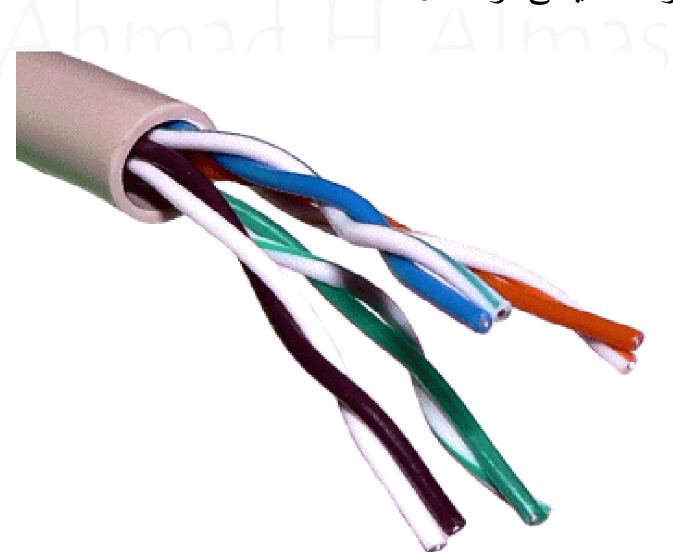
- يوجد نوعان من الكابل المحوري :

- **Thick net** هذا النوع السميك و قوي من نوعه و يدعم مسافة أكبر من الـ **Thin net**.
- **Thin net** هذا النوع النحيف قوي ايضاً ولكن المسافة أقصر من الـ **Thick net.**

المسافة ٥٠٠ متر السرعة ١٠**mbps** هذا النوع يدعم الـ **Thick**

المسافة ٣٠٠ متر السرعة ١٠**mbps** هذا النوع يدعم الـ **Thin**

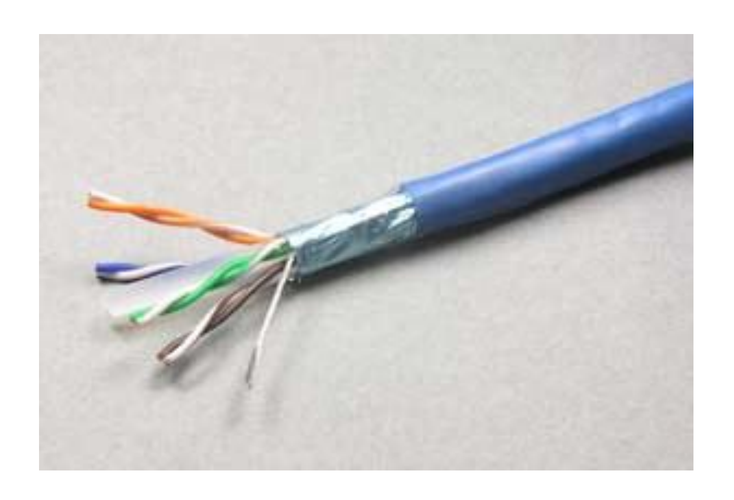
٢- **Twisted Pair Cable :** يتكون هذا النوع من الاسلاك من عدد من الأزواج الملفوفة على بعضها كما بالصورة التالية وهذا الالتفاف يعمل على تقليل التشويش أو التداخل الكهرومغناطيسى نوعاما.



وينقسم هذا النوع إلى قسمين :

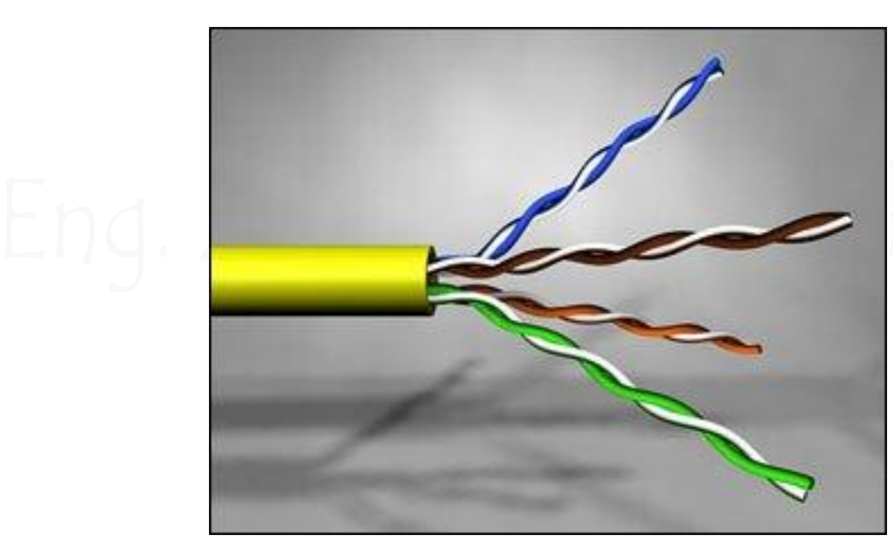
١- الكابلات الثنائية الملفوفة المحمية **Shielded Twisted Pair / STP**

وهي عبارة عن أزواج من الأسلاك الملتوية محمية بطبقة من القصدير ثم بغلاف بلاستيكي خارجي كما بالصورة التالية .



٢-الكابلات الثنائية الملفوفة الغير محمية **Unshielded Twisted Pair / UTP**

وهي تتكون من أسلاك ملتوية داخل غطاء بلاستيكي بسيط ،وقد صنفت جميعة الصناعات الإلكترونية كيابل الـ **UTP** إلى **6** فئات مشهورة هي :



Cat 1 هذه الفئه تستخدم لنقل الصوت فقط و لا تستخدم لنقل البيانات

Cat2 هذه الفئه تستخدم لنقل البيانات بسرعه تصل إلى **4** ميجابت.

Cat3 هذه الفئه تستخدم لنقل البيانات بسرعة تصل إلى **10** ميجابت.

Cat4 هذه الفئه تستخدم لنقل البيانات بسرعة تصل إلى **16** ميجابت.

Cat5 هذه الفئه تستخدم لنقل البيانات بسرعة تصل إلى **100** ميجابت.

Cat5 هذه الفئه تستخدم لنقل البيانات بسرعة قد تصل إلى **1000** ميجابت اعتمادا على طول السلك و نوعية السوتش.

Cat6 هذه الفئه تستخدم لنقل البيانات بسرعة تصل إلى **1000** ميجابت و أكثر.

وكان ذلك قبل أن تظهر الفئة السادسة **Category 6** والتي تستخدم لنقل البيانات بسرعة ١ جيجابايت في الثانية.

و تتفوق كابلات STP على UTP في أمرين :

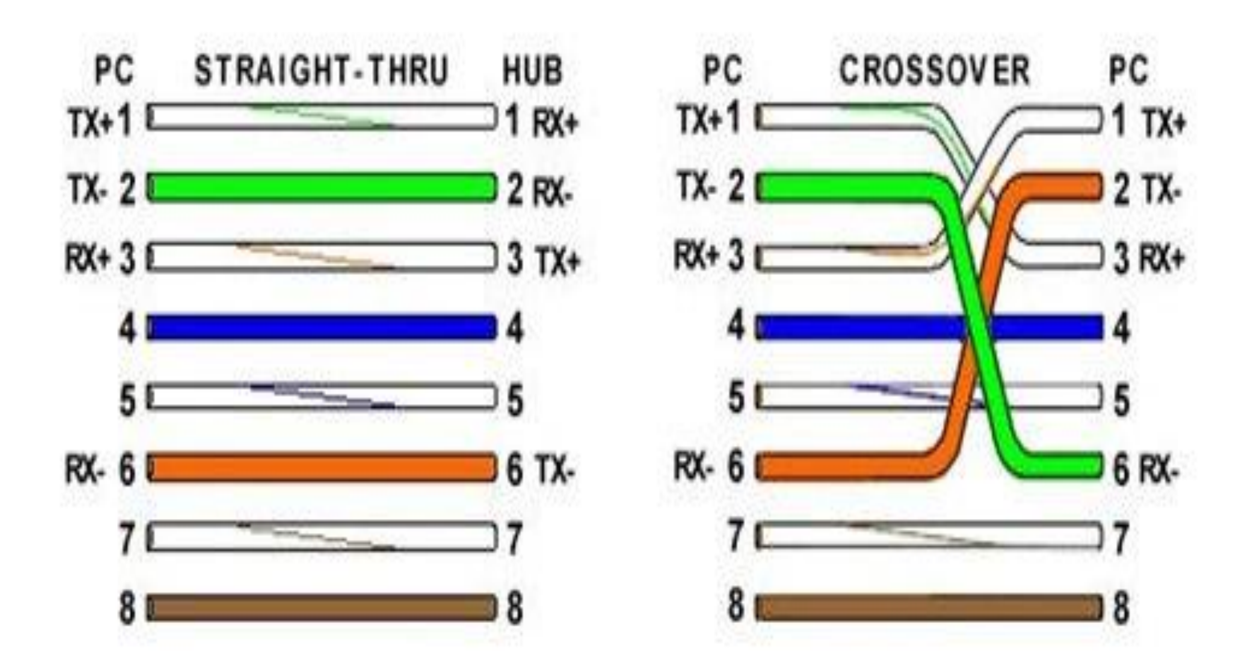
- أقل عرضة للتداخل الكهرومغناطيسي.
- تستطيع دعم الإرسال لمسافات أبعد.
- في بعض الظروف توفر سرعات بث أكبر.
- و تستخدم الكابلات الملتوية **UTP** عادة في الحالات التالية:
- عندما ا يكون هناك الحاجة إلى ميزانية محدودة للشبكة.
- وعندما ا يكون هناك حاجة لتوفير سهولة و بساطة في التركيب.

هناك نوعين من التوصيل فى الكابل STP و UTP :

التوصيل المباشر (**Straight cable**) و هو يستخدم لتوصيل أجهزة مختلفة مثل كمبيوتر مع سويتش

والتوصيل التقاطعي (**Crossover cable**) و هو يستخدم لتوصيل أجهزة متشابهه مثل سويتش مع سويتش

وهذه صورة ترتيب الاسلك في داخل الـ Rj-45 من النوعين الخاصين في التوصيل :

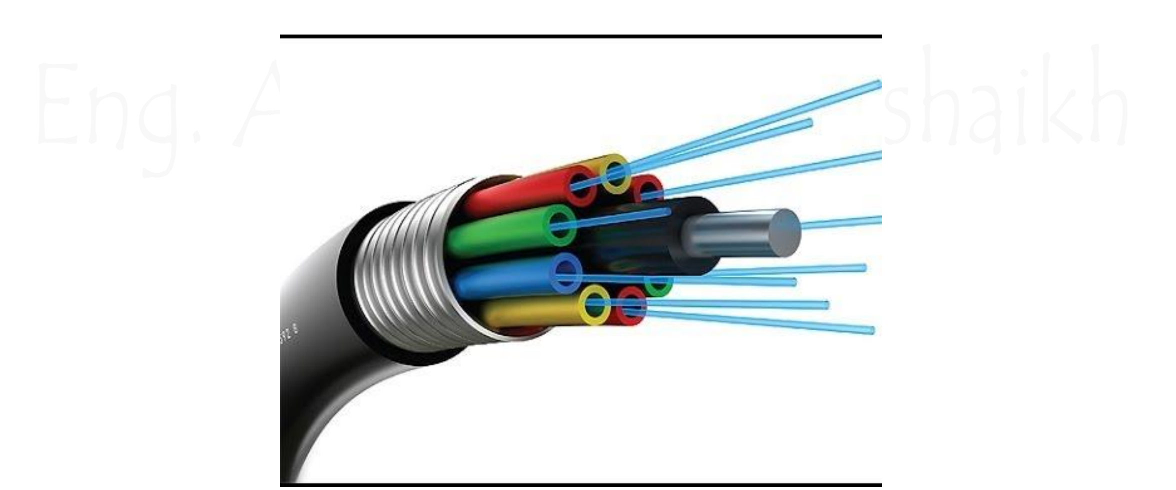


تستخدم الكابلات STP و UTP مشبك من نوع RJ- 45



٣- كابلات الالياف البصرية fiber optic cables :

كابلات الألياف البصرية تستخدم فى نقل البيانات فى شكل اشارات ضوئية ، وهي ألياف مصنوعة من الزجاج النقي طويلة ورفيعة لا يتعدى سمكها سمك الشعرة يجمع العديد من هذه الألياف في حزم داخل الكيبلات البصرية وتستخدم في نقل الإشارات الضوئية لمسافات بعيدة جداً.



وتتكون من ثلاث طبقات كما بالصورة السابقة :

١- طبقة القلب **Core** : وهى عبارة عن الياف من الزجاج أو البلاستيك ينتقل فيه الضوء.

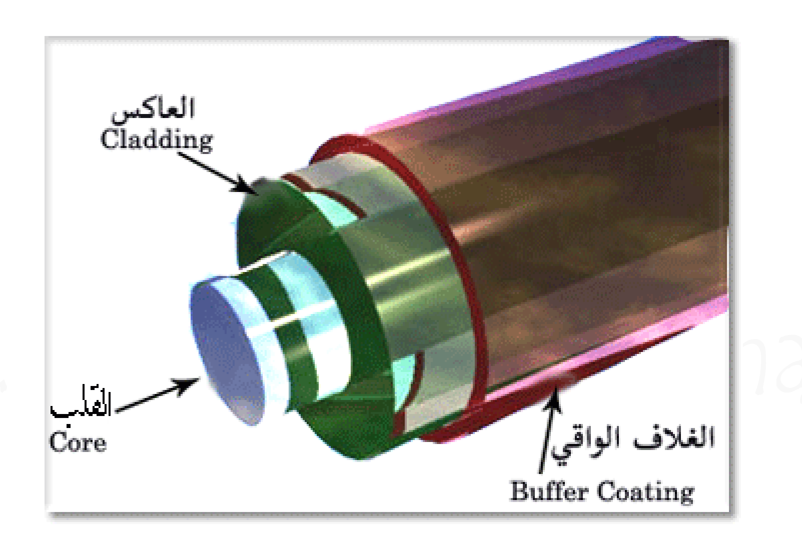
٢- الصميم أو العاكس **Cladding** : مادة تحيط باللب الزجاجي وتعمل على عكس الضوء مرة أخرى إلى مركز الليف البصري.

٣- الغلاف الواقي **Buffer coating** : وهى طبقة تستخدم لحماية الكابل من التغيرات الجوية أو الكسر.

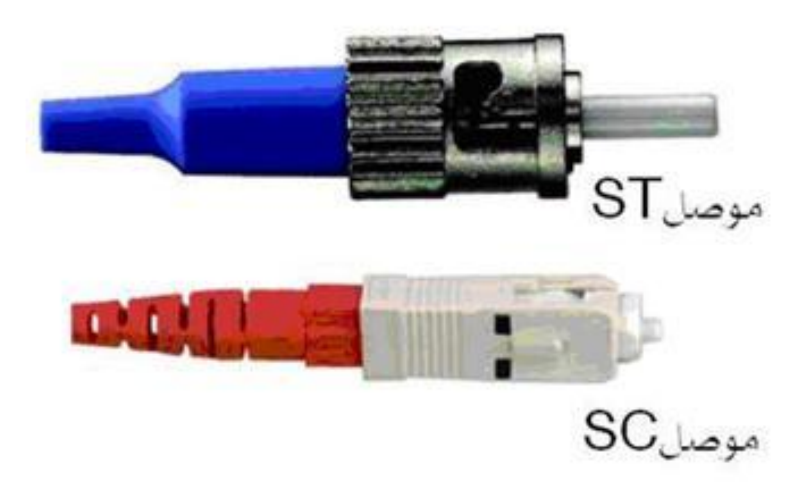
توفر أسلاك الألياف البصرية المزايا التالية :

- منيعة ضد التداخل الكهرومغناطيسي و التداخل من الأسلاك المجاورة.
- معدلات التوهين منخفضة جدا.
- سرعة إرسال بيانات مرتفعة جدا بدأت ب **100** ميجابت في الثانية و قد وصلت حاليا إلى **200000** ميجابت في الثانية.

- في الألياف البصرية يتم تحويل البيانات الرقمية إلى نبضات من الضوء، و حيث أنه لا يمر بهذه الألياف أي إشارات كهربائية فإن مستوى الأمن الذي تقدمه ضد التنصت يكون مرتفعا.



يستخدم حاليا نوعان من منفذ التوصيل كما في الصورة



أنواع الألياف الضوئية

الألياف الضوئية يمكن أن تقسم بصفة عامة إلى نوعين أساسيين:

الآلياف الضوئية ذات النمط الاحادي **single mode fiber** تنتقل من خلالها إشارة ضوئية واحدة فقط في كل ليفة ضوئية من ألياف الحزمة وهي النوع الأسرع نقلا للبيانات وتستخدم في شبكات التلفون و كوابل التلفزيون.
هذا النوع من الألياف يتميز بصغر نصف قطر القلب الزجاجي حيث يصل إلى حوالي **9 micron** حيث **1** ميكرومتر تساوي **0,001** ملليمتر و تمر من خلاله أشعة الليزر تحت الحمراء ذات الطول الموجي ١.٣-١.٥٥ nm.
الآلياف الضوئية ذات النمط المتعدد **multi -mode fibers** و بها يتم نقل العديد من الإشارات الضوئية من خلال الليفة الضوئية الواحدة مما يجعل استخدامها أفضل لشبكات الحاسوب. هذا النوع من الألياف يكون نصف قطره اكبر حيث يصل إلى **٦٢.٥ micron** و تنتقل من خلاله الأشعة تحت الحمراء.

مميزات الألياف البصرية :

١- سريعة جدا في نقل البيانات حيث بدأت بـ (**100** ميجابت/ث) وقد وصلت حاليا إلى أكثر من **200,00** ميجابت/ث.

٢- مستوى الأمن التي تقدمه ضد التنصت عالية جدا لأنها تقوم بتحويل البيانات الرقمية إلى نبضات ضوئية فلا يمر بهذه الألياف أي إشارات كهربائية.

٣- معدل انخفاض الإشارات منخفضة بشكل كبير مهما كانت طول السلك.

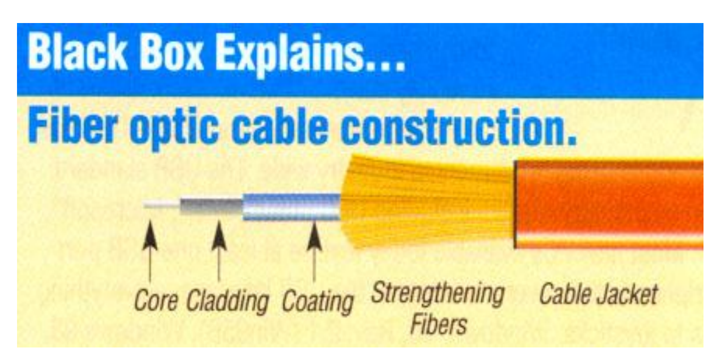
٤- منيع ضد التداخل الكهرومغناطيسي التي تؤدي إلى تشويش الإشارات.

ولهذا يمكن تمديد هذا الألياف على شكل كابلات كبيرة تحتوي على آلآف الأسلاك بداخلها دون أن تؤثر على جودة الاتصال.

٥- يمكن تمديد عدة ألياف بصرية بداخل كابل واحد مما يسهل عملية التركيب.
٦- لا تتأثر بالماء بل أصبح الدول تستخدمها لتوصيل الانترنت بين المحيطات.

أما العيب الرئيسي في هذه الكابلات أو الأسلاك :

العيب الوحيد هو أنها صعبة التركيب والصيانة ولأنها تعتمد على الزجاج فغالبا ما تنكسر النواة الزجاجي عند الانحنائات الشديدة إلا تلك المصنوعة حديثا من نواة بلاستيكية لكنها لا تستطيع حمل نبضات الضوء مسافات شاسعة كتلك المزودة بقالب زجاجي .



البروتوكولات Protocols

- سنقوم بذكر بعض البروتوكولات المهمة جداً التي يجب أن نتعرف عليها ما قبل التعمق في عالم الشبكات، سنقوم بذكر البروتوكولات و شرح بسيط عن كل نوع و ما هي وظيفة كل بروتوكول .

- في البداية يجب أن نعلم أن كل بروتوكول يأخذ منفذ **Port** يعمل عليه وتبدأ هذه المنافذ من **0** حتى **65535** منفذ، و يجب أن نعلم أيضاً إنه يوجد بعض المنافذ المحجوزة لبعض البروتوكولات وتبدأ هذه المنافذ المحجوزة من **0** حتى **1024 Port** لا نستطيع العمل عليهم لأنهم محجوزين للبروتوكولات .

DNS - Domain Name System:

نظام أسماء النطاقات هو نظام يخزن معلومات تتعلق بأسماء نطاقات في قاعدة بيانات موزعة على الإنترنت يقوم خادم اسم النطاق بربط العديد من المعلومات بأسماء النطاقات، ولكن وعلى وجه الخصوص يخزن عنوان **IP** المرتبط بذلك النطاق، بمعنى آخر هو نظام يقوم بترجمة أسماء النطاقات من كلمات إلى أرقام تعرف باسم عنوان الـ **IP** .

DHCP - Dynamic Host Configuration Protocol:

يستخدم هذا البروتوكول لإسناد عناوين **IP** بشكل آلي لحواسب مضيفة **Hosts** أو محطات عمل **Workstation** على شبكة **TCP/IP**، وبذلك نتجنب حالات التضارب في عناوين **(IP address conflict)** والتي تحدث نتيجة استخدام نفس عنوان **IP** لأكثر من جهاز على الشبكة (عند إسناد العناوين بشكل يدوي) مما يؤدي إلى فصل بعض الأجهزة عن الشبكة، فهذا البروتوكول نظام لاكتشاف العناوين المستخدمة مسبقا.

SNMP - Simple Network Management Protocol:

بروتوكول إدارة الشبكات البسيط، هو جزء من حزمة مواثيق بروتوكولات الإنترنت بحسب تعريف **IETF** وبشكل أكثر تفصيلاً، هو أحد مواثيق (بروتوكولات) الطبقة السابعة، أو طبقة التطبيقات المستخدمة من نظام إدارة الشبكات لمراقبة الأجهزة الموصولة بالشبكة للظروف التي تحتاج إلى انتباه من مدير النظام.

NTP - Network Time Protocol:

هو بروتوكول يقوم بتوزيع التوقيت العالمي المنسق عن طريق مزامنة ساعات الحواسب الالية المرتبطة معا بشبكة واحدة. يستخدم بروتوكول وقت الشبكة المنفذ رقم **123** من بروتوكول وحدة بيانات المستخدم **UDP**.

FTP - File Transfer Protocol:

بروتوكول نقل الملفات، المستخدم في نقل الملفات بين أجهزة الحاسوب سواء من حاسوب إلى حاسوب أو من حاسوب إلى خادم.

:POP - Post Office Protocol

هو نظام بريد يعمل في طبقة البرامج، ويهدف إلى جلب رسائل البريد الإلكتروني ليعمل ما من خوادم **POP** .

:SMTP - Simple Mail Transfer Protocol

هو المعيار الأساسي لإرسال البريد الإلكتروني عبر الإنترنت واليوم يستعمل تطوير له باسم **ESMTP** اختصاراً لـ **Extended SMTP**

:SSL - Secure Sockets Layer

بروتوكول طبقة المنافذ الآمنة **Secure Socket Layer** اختصار **SSL** يتضمن مستوى عال من الأمن في نظام تسلسل البروتوكولات الهرمي.

:HTTPS - Secure HTTP

بروتوكول نقل النص التشعبي الآمن (**HTTPS**)هو مزيج من بروتوكول نقل النص التشعبي مع خدمة تصميم المواقع تلس / بروتوكول لتوفير الاتصالات المشفرة وتحديد تأمين شبكة خادم الويب. غالبا ما تستخدم الشبكي وصلات لمعاملات الدفع على الشبكة العالمية للمعاملات ونظم المعلومات الحساسة في الشركات. الشبكي لا ينبغي الخلط بينه وبين النص المتشعب الآمن .

:HTTP - Hyper Text Transfer Protocol

هو نظام نقل مواد الإنترنت عبر الشبكة العنكبوتية الويب، وهو الطريقة الرئيسة والأكثر انتشاراً لنقل البيانات في الويب(**www**) الهدف الأساسي من بنائه كان إيجاد طريقة لنشر واستقبال صفحات **HTML** .

:IP - Internet Protocol

بروتوكول الإنترنت **IP** ، ميثاق الإنترنت أو ميفاق الإنترنت، هو بروتوكول يعمل على الطبقة الثالثة طبقة الشبكة (**Network Layer**) من نموذج **osi**، يحدد كيفية تقسيم المعلومة الواحدة إلى أجزاء أصغر تسمى رزما(**packet**) ، ثم يقوم الطرف المرسل بإرسال الرزمة إلى جهاز آخر مسير على الشبكة يستخدم نفس الميثاق البروتوكول.

:LDAP - Lightweight Directory Access Protocol

هو اختصار لـ **Lightweight Directory Access Protocol** وترجمتها البروتوكول الخفيف للوصول للدليل هو بروتوكول يستخدم في شبكات الحاسوب للاستفسار عن وتعديل خدمات الأدلة العاملة فوق بروتوكول **TCP/IP** بحيث يمكن لخدمات مثل عميل البريد الإلكتروني وغيره استخدامها للتحكم بدخول المستخدمين.

:. ICMP - Internet Control Message Protocol

هو بروتوكول يعمل ، ويعمل في داخله بروتوكول الـ **Ping** وهو اختصار لـ **Packet Internet Groper** وهو يعتبر من أهم البروتوكولات المستخدمة ولا أحد يستطيع الاستغناء عنه في عملية استكشاف المشاكل **Troubleshoot** ووظيفة هذا البروتوكول التأكد من سلامة الاتصال ما بين الاجهزة المتصلة مع بعضها البعض على الشبكة ومن خلال عملية الـ **Ping** يتم إرسال أربعة **Packets** بحجم **32 bit** بشكل **Echo Packet** الى الجهة المطلوبة وسيتم الرد بمثل هذه البكت من الجهة المطلوبة لنتأكد هل الجهاز متصل على الشبكة أم لا .

:ARP - Address Resolution Protocol

بروتوكول تحليل العناوين **Address Resolution Protocol** وكثيراً ما يشار إليه بإختصار (**ARP**) هو بروتوكول الاتصالات السلكية واللاسلكية المستخدمة لتحليل عناوين بطقة الشبكة إلى عناوين طبقة الارتباط، وظيفة هامة في شبكات اتصال متعددة-الوصول .

:RARP - Reverse Address Resolution Protocol

بروتوكول إيجاد العناوين المعكوس (**Reverse ARP : RARP**) يقوم هذا البروتوكول بالوظيفة المعاكسة لوظيفة الـ **ARP** وهو يمكن النظام من إيجاد العنوان المنطقي خاصته عن طريق إرسال العنوان الفيزيائي لمخدم **RARP** .

:PPTP - Point to Point Tunneling Protocol

PPP اختصار لكلمة **Point to Point Protocol** ويعني بروتوكول النقطة إلى النقطة وهو وسيلة فعالة تسمح لحاسوب بعيد بالاتصال بالشبكة. يوجد هذا البروتوكول في طبقة الربط (**Data Layer**) في حزمة بروتوكولات الإنترنت **TCP/IP** .

:TCP - Transmission Control Protocol

ميفاق التحكم بالنقل جزء أساسي من حزمة بروتوكولات الإنترنت حيث يمثل هو والميفاق **IP** أولى موافيق هذه الحزمة، لذلك يرمز لهذه الحزمة بالرمز تي سي بي/آي بي .(**TCP/IP**)

:UDP -User Datagram Protocol

هو واحد من الأعضاء الرئيسية لمجموعة بروتوكول الإنترنت وهي مجموعة من بروتوكولات الشبكات التي تستخدم للإنترنت.

OSI

Open Systems Interconnection

OSI : هى مراحل تكون الداتا أو البيانات ونقلها من الـ **Source device** جهاز المرسل إلى جهاز المستقبل **Destination device**.

وهو نظام في مجال شبكات الحاسوب المرجع الأساسي لترابط الأنظمة المفتوحة .

المرجع وضعته المنظمة الدولية للمعايير (**ISO**) سنة **1983** برقم **7498** ، ليكون نموذج نظري موثوق لبروتوكولات الاتصالات بين الشبكات الحاسوبية.

المهام : وظائف الاتصال والتنظيم حسب مرجع أو إس آي مقسمة على سبع طبقات (**Layers**) مختلفة.

لكل طبقة دور يضم مجموعة مهمات يتطلب تحقيقها داخلها وعبر التواصل مع الطبقة التي تسبقها أو التي تليها حسب الترتيب.

ويشرح مرجع أو إس آي ذلك من خلال ٤ أجزاء هي :

- النموذج القاعدي
- نظام الحماية
- التسمية والعنونة
- الإطار العام للتسيير(**Routing**)

تم مراجعة المرجع سنة **1994** بتركيز على الجزء الأول.

يوصف المرجع على أنه نظري. ذلك أن المرجع يصف بشكل عام المهام والأدوار التي تقوم بها أنظمة الربط الشبكية من دون الدخول في التفاصيل التقنية أو ذكر للتكنولوجيات المستعملة. بعض تفصيل المرجع من حيث العمليات والوظائف لم يتم لحد الآن دمجها في أحد من الأنظمة.

الأهداف :

١. ضمان نقل البيانات عبر الشبكة بطريقة امنة وسليمة.
٢. توفير نفقات عرض الحزمة الدولي.
٣. توفير جودة أفضل لخدمة نقل الصوت عبر بروتوكول الإنترنت.**VoIP**
٤. إدارة الخدمة وتوسّع الشبكة.

مميزات OSI :

Provides a standard for hardware development

بمعنى إنها توفر توحيد قياس ثابت يستخدمه مطورون أجهزة الهاردوير للشبكات

Allows for modular software development

توفر لمطورى برامج السوفت وير التركيز على طبقة واحدة والتى سيعمل عليها البرنامج أو إذا كان سيعمل على عدة طبقات مختلفة حسب الوظيفة التى سيقوم بها

Speed development of new technology

تجعل عملية تطوير كل ما هو متعلق بالشبكات سريعة

فائدة فهم OSI Layers :

١- تستطيع فهم و حل المشاكل **Troubleshooting** الشبكات.

٢- معرفة كيفية تكوين الداتا وما هو شكلها فى كل مرحلة **Encapsulations** .

٣- بعد أن تفهم الطبقات أو مراحل ال **OSI** وكيف تتكون البيانات خلالها تستطيع أن تفهم وتحل المشاكل التى تصادفك على الشبكة،فعندما ا تعرف كل جهاز أو هاردوير أو حتى تطبيق أو بروتوكول أين يعمل وفى أى مرحلة فعندها تستطيع التوصل لحل المشكلة بطريقة أسرع ، فعلى سبييل المثال عندما ا تقوم بعمل **Ping** على جهاز آخر على الشبكة فتفشل العملية فعلى اى اساس تصل لسبب المشكلة فهناك عدة اسباب قد تكون احدهما سبب المشكلة مثل الكابل أو كارت الشبكة أو بروتوكول **Tcp/ip** فعندما ا تفهم طبقات **OSI** ستعرف أن كل منهم يعمل فى طبقة ولهذا ينصح بالكشف أولا عن الكابل الطبقة الأولى **physical** ثم كارت الشبكة الطبقة الثانية **data link** (ثم **Tcp**) .

٤- معرفة و تتبع كل شيء في الشبكة من خلل الـ **OSI** و معرفة كل طبقة ماذا تقوم في وقت الإرسال و الاستقبال و تتبع البيانات المرسلة و المستقبلة من و إلى المستخدم .

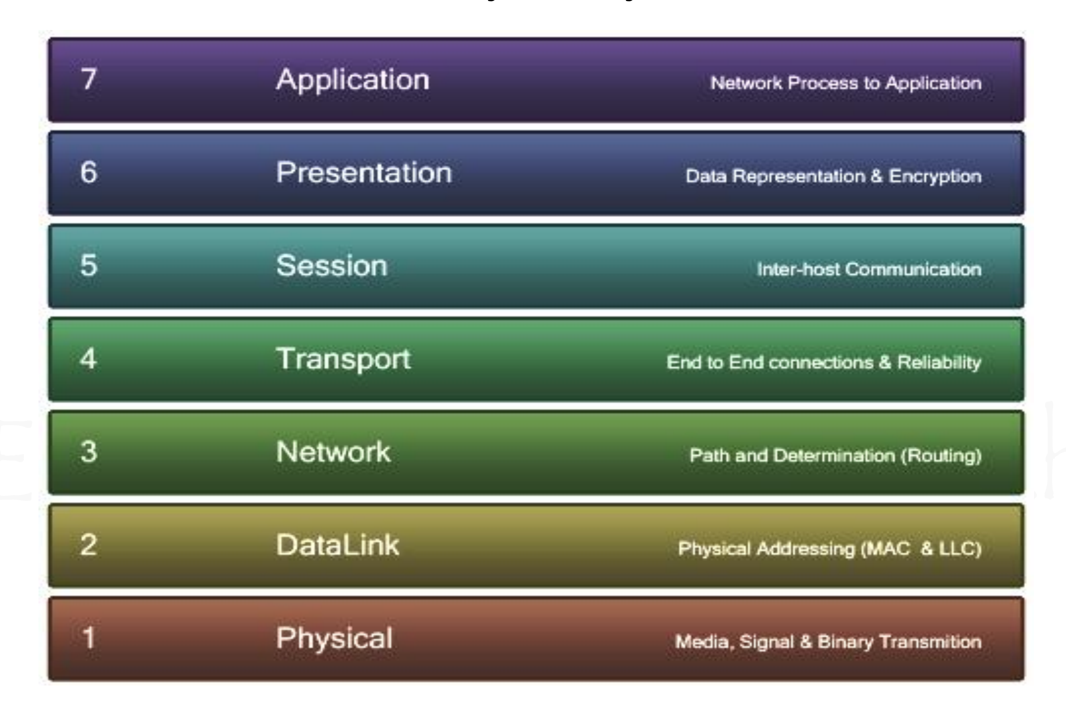
٥- تفيد بمعرفة النقاط الحساسة في الشبكات و اخذ الحذر منه و كيفية تشفير الدتا و فك التشفير .

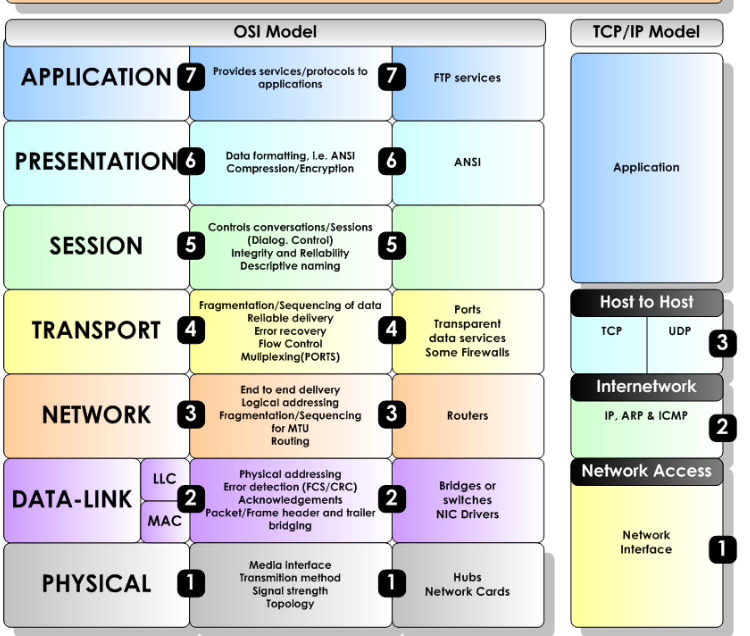
٦- معرفة كل جهاز في اية طبقة يعمل مثل الهاب و الراوتر و السويتش و جهاز الكمبيوتر.

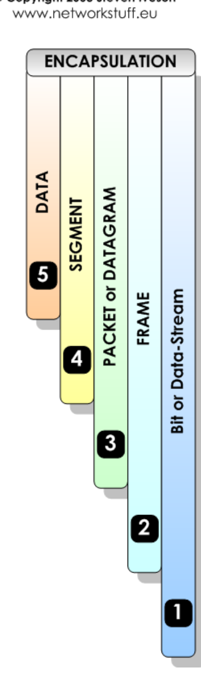
Layer	Name	description - task
7	Application	Implementation of the OS environment - user
6	Presentation	Formatting and presentation of data - ASCII code, etc.
5	Session	Harmonization opportunities of of various systems
4	Transport	Control over the transfer of data - correctness
3	Network	Control the flow in the network and between networks
2	Data Link	Rules of exchange - packing and sending data
1	Physical	Electrical and physical connections - wiring

طبقات المرجع : يعرض مرجع أو إس آي على شكل 7 طبقات (التي تتكون) بشكل عمودي، أعلاه الطبقة السابعة وأسفله الطبقة الأولى.

7- Application layer
6- Presentation layer
5- Session layer
4- Transport layer
3- Network layer
2- Data link layer
1- Physical layer







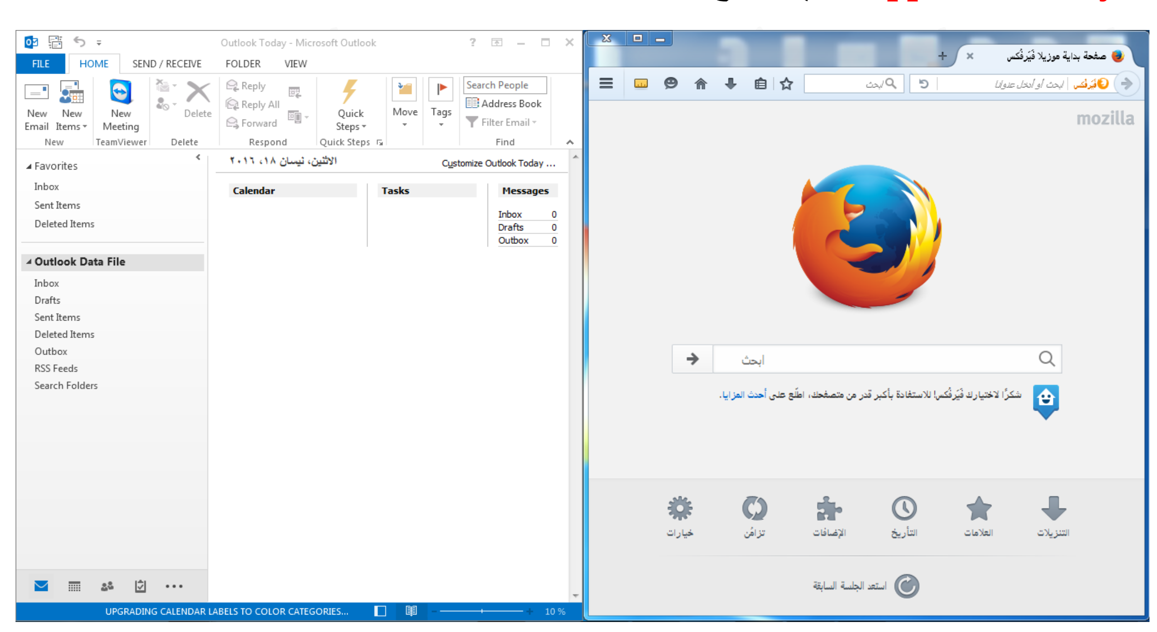
شرح مراحل كل طبقة من طبقة OSI Layer بالتفصيل :

سأقوم بشرح كل طبقة بالتفصيل مع ذكر بعض الامثلة على كل طبقة و معرفة كل طبقة و ما هي وظيفتها .

7- Application layer

هذه الطبقة المسؤولة عن التطبيقات مثل البرامج التي يتعامل معها المستخدم مثل تصفح الانترنت يحتاج الى البرامج مثل برامج التصفح **Google Chrome** أو **Mozilla Firefox** أو عندما يريد رفع ملفات إلى السيرفر أو سحب ملفات يحتاج ايضاً إلى برامج النقل مثل **FTP Client** أو عندما ا يحتاج لـ إرسال بريد أو استقبال بريد يحتاج برنامج **Outlook** كل هذه البرامج تعمل في طبقة التطبيقات – **Application layer** بمعنى ما يتم العمل عليه من قبل المستخدم بشكل تطبيق كله يندرج تحت طبقة الـ **Application layer** و بطبع كل هذه البرامج تحتاج لـ البروتوكولات و سأقوم بذكر بعض من هذه البروتوكولات التي تعمل في طبقة التطبيقات – **Application layer** .

في هذه الصورة يوجد برنامج الـ **Mozilla Firefox** و برنامج الـ **Outlook** في هذه المرحلة يجب المعرفة اننا الأن نقف في الطبقة السابعة و هي طبقة التطبيقات **Application layer** واي برامج اخرى .



(**Application**)

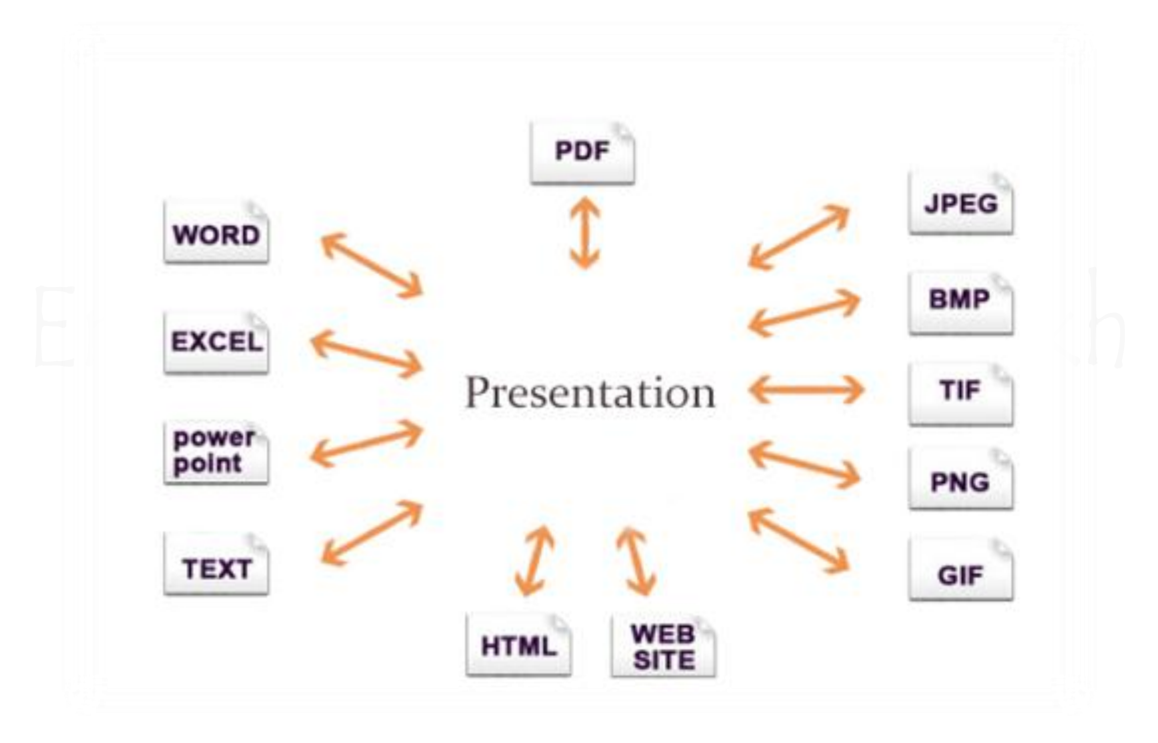
البروتوكولات التي تعمل في طبقة التطبيقات - **Application layer** :

SNMP , DNS , FTP , LDAP , LMP , NTP , HTTP , DHCP , Open VPN , SMTP , POP3 , IMAP , WAE , WAP , SSH, Telnet , SIP , PKI , SOAP , rlogin , TLS / SSL .

6- Presentation layer

هذه طبقة العرض الطبقة المسؤولة عن تهيئة البيانات و التفريق ما بين كل نوع من البيانات و في هذه الطبقة يتم العمل على اعداد و اخذ كل امتداد على حسب نوع البيانات مثل النصوص و الصور و الفيديو و الملفات المضغوطة و تقوم هذه الطبقة بعمل تشفير و فك التشفير للبيانات و تقوم بتغيير شكل البيانات إلى أشكال مختلفة إذا تطلب الأمر و بعد أن تتم عملية التهيئة سيتم الإرسال من جهاز المرسل إلى جهاز المستقبل و العكس .

مثال على طبقة العرض تقوم طبقة العرض بعمل الصيغ المناسبة للبيانات مثل عندما نقوم بإرسال صورة ستقوم الصورة بنزول من طبقة التطبيقات و هي الـ **Application layer** و الوصول إلى طبقة العرض **Presentation layer** و عند الوصول لهذه الطبقة ستقوم بعملية تهيئة الصورة و وضع الصيغة التالية إذا كانت صورة الصيغة **png , jpeg , gif** في هذه المرحلة سيتم تحديد نوع الصورة و إرساله بصيغتها .



Presentation layer

البروتوكولات التي تعمل في طبقة العرض - **Presentation layer** :

JPEG , MPEG , ASCII , EBCDIC , HTML , AFP , PAD , NDR , RDP , PAD , AVI .

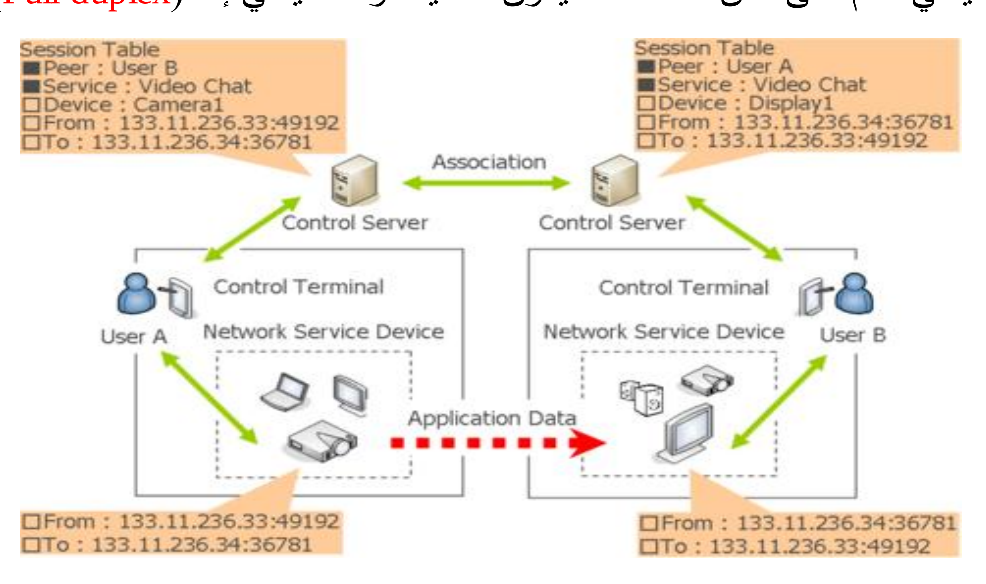
عملية التهيئة : هي عملية تهيئة البيانات أو الداتا ليتم اخذ صيغتها و امتداها المناسب .

عملية الضغط و فك الضغط : هي عملية ضغط البيانات من قبل المرسل حتى تصل المستقبل و عند استلم البيانات للمستبقل سيتم فك الضغط و كذلك عملية التشفير و فك التشفير .

5- Session layer

هي الطبقة المسؤولة عن جلسة العمل و عن ادارة و فتح و اغلاق اية اتصال ما بين المستخدمين و مثال على ذالك عندما نقوم بفتح أكثر من موقع على شبكة الانترنت نقوم بدخول على المتصفح و نقوم بدخول على أكثر من موقع في نفس الوقت و من غير اية مشكلة هذا لي إنه طبقة الـ **Session** تقوم بادارة الاتصال و تنظيمها بينم تقوم ايضاً هذه البطقة بفتح كل بورت لكل تطبيق معين مثل انا الأن اتصفح موقع فيس بوك و اريد الدخول إلى موقع جوجل و يوتويب في نفس الوقت لا يوجد اية مشكلة سأقوم بدخول عليهم بكل سهولة وذلك لي أن طبقة الـ **Session** تقوم بفتح بورت لكل موقع لوحده و ايضاً هذه الطبقة تقوم بتحدد نوع الاتصال المستخدم مثل الإرسال في اتجاه واحد (**single**) هذا يعني الإرسال في اتجاه واحد يرسل مره واحد مثل الراديو و التلفزيون تسمع ولا تسطيع الرد عليه و يجد ايضاً الإرسال و الاستقبال في نفس الوقت (**half duplex**) هذا يعني الإرسال و الاستقبال في نفس الوقت ولكن بشكل متقطع مثل عند وصول الإشارة للطرف الآخر سيتم الاستقبال و عند استقبال الإشارة و قبولها يستطيع الإرسال مره آخر من المستقبل إلى المرسل ولكن بشكل مرتب و منظم من دون تداخل الإشارة , و يوجد النوع الاخير من أنواع الإرسال

(**Full duplex**) هذا النوع من الاتصال يكون بشكل مباشرة استقال و إرسال بخط واحد من دون انتظار بمعنى يستقبل و يرسل في نفس الوقت على خط واحد من دون تقطع مثل عندما تكون تتصل على أحد الاصدقاء و تتكلم معه على الهاتف لحظة انك تسطيع مقطعته و الحديث معه و هو في نفس الحظة يتكلم و انتا في نفس هذه الحظة تتكلم هذه يعني انكم على نفس الخط تستطيعون الحديث و هذه يعني إنه (Full duplex)

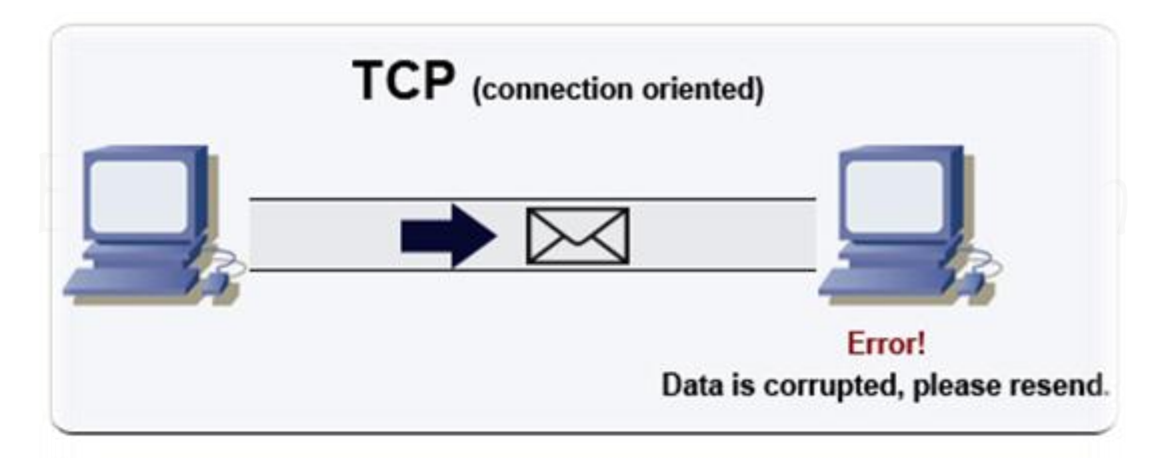


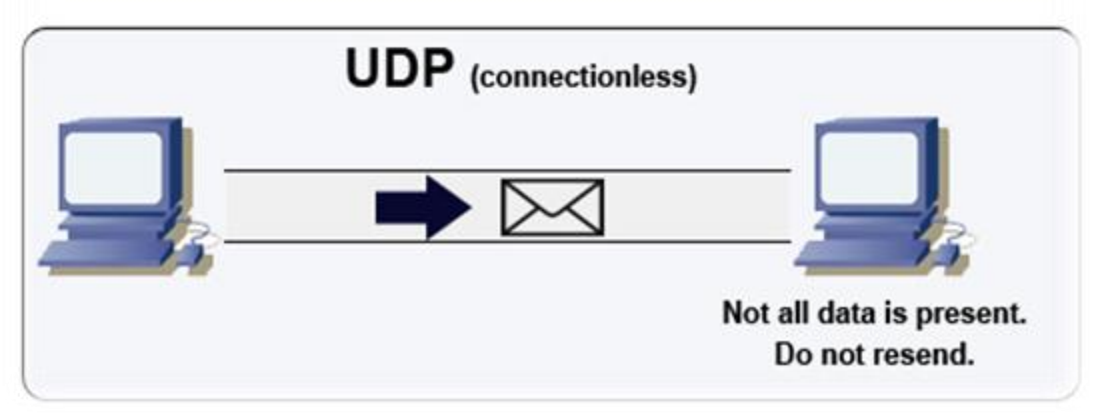
البروتوكولات التي تعمل في الطبقة المسؤولة عن جلسة العمل - **Session layer :**

SAP, RTP, NFS, SQL, RPC, NETBIOS NAM, NCP, SOCKETS, SMB, NETBEUI, 9P.

4-Transport layer

هذه الطبقة المسؤولة عن نقل و ادارة البيانات و تحديد نوع البيانات المرسلة و المستقبلة وبعده تقوم بتحديد نوع البروتوكول المناسب للبيانات في عملية إرسال و نقل البيانات مثل بعض البيانات تحتاج استخدام بروتوكول **TCP Connection oriented protocol** هذا البروتوكول يستخدم في في نقل البيانات المهمة جداً هذا البروتوكول بعد نقل البيانات يتاكد من وصول البيانات بشكل كامل و إذا لم يتم توصيل البيانات بشكل كامل سيقوم بعودة إرسالة مره اخرى و يوجد عملية تقوم بهذه المهمة سأقوم بشرحها في نهاية هذا الموضوع , اما البيانات التي تستخدم بروتوكول الـ **UDP Connectionless** هي البيانات تكون مثل الصوت و الفيديو مثل عندما تستخدم برنامج السكايب بعض اوقت تشعر أن الصوت أو الصورة يوجد فيهم تقطع و عدم وضوح للصوت و الصورة لماذا لإنه هذه البيانات يتم نقلها عن طريق بروتوكول الـ **UDP** و هذا البروتوكول لا يهتم في توصيل البيانات بشكل كامل فقط ينقل مره واحدة و لا يتاكد من البيانات هل تم استلامه بشكل كامل أو لا لهذا السبب ترى الصوت أو الصورة يوجد فيها ضعف و تقطيع على عكس بروتوكول الـ **TCP** فهو يتاكد من وصول البيانات بشكل كامل .





البروتوكولات التي تعمل في الطبقة المسؤول عن نقل و ادارة البيانات - Transport layer

TCP: Transmission Communication Protocol

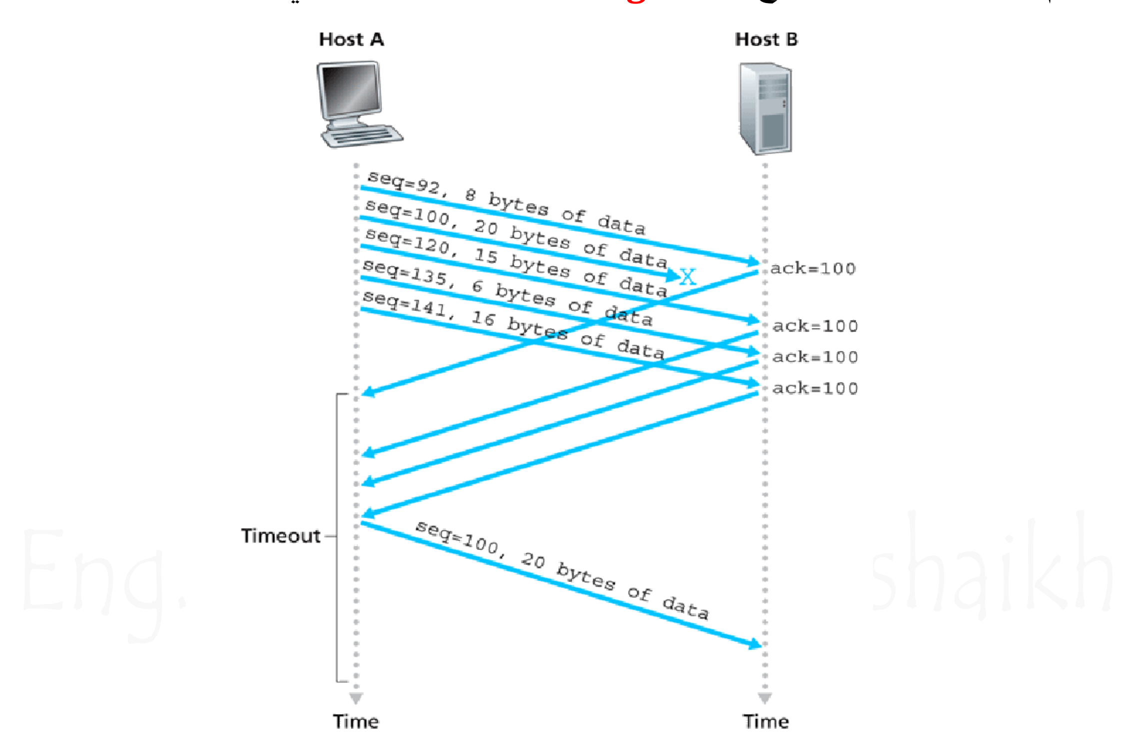
UDP: User Datagram Protocol

طريقة التحكم في نقل البيانات في طبقة النقل **Transport layer** :

يوجد طريقتان للتحكم في عملية نقل البيانات .

١- التحكم في نقل البيانات **flow control** , و تصحيح الاخطاء **Error correction**

تتم عليمة نقل البيانات **flow control** عن طريق تقطيع الداتا ثم ترقيمها **Sequencing** ثم الإرسال و التأكد من الطرف الآخر بالإستلام وقته يقوم الطرف الآخر برد على إنه استلام البيانات بشكل صحيح **Acknowledgments** إرسال باقي الداتا .



Flow-control

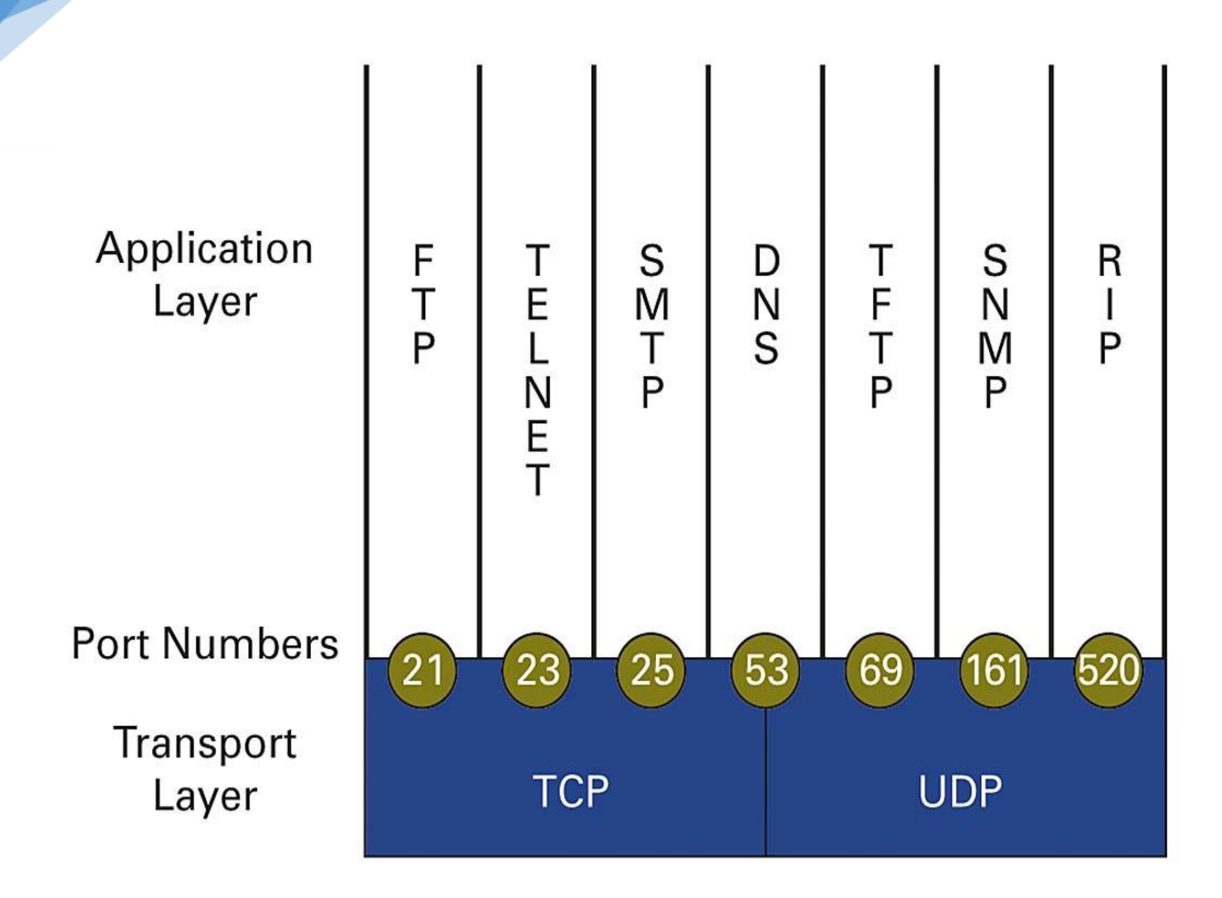
٢- يتم تحديد نوع البيانات و بعده يتم تحديد نوع البروتوكول الذي يجب استخدامه **TCP or UDP** .

٣- بعده سيتم اختيار البورتات المناسبة لكل تطبيق .

يوجد نوعان من البورتات :-

- البورتات المحجوزة تكون هذه البورتات محجوزة في داخل النظام لبعض التطبيقات و البروتوكولات و تبداء هذه البروتوكولات من (**0 to 1024**) و هذه البروتوكولات لا يمكن استخدامها على تطبيقات اخرى .

- البورتات الآخر و تستخدم هذه البورتات من قبل التطبيقات التي يتم العمل عليه على النظام مثل البرامج مثل برنامج المتصفح أو برنامج السكايب أو برنامج الريموت كنترول أو برنامج التحكم عن بعد و هذه التطبيقات تقوم باخذ بورتات بشكل عشوائي للخروج على الشبكة للوصل إلى جهاز اخرى ليدخل من بورت مختلف .



OSI Model Layers

Application Layer
Presentation Layer
Session Layer
Transport Layer
Network Layer
Data-Link Layer
Physical Layer

TCP/IP Protocol Architecture Layers

Application Layer
Host-to-Host Transport Layer
Internet Layer
Network Interface Layer

TCP/IP Protocol Suite

Telnet FTP SMTP DNS RIP SNMP
TCP UDP
IGMP ICMP
IP
ARP
Ethernet
Token Ring
Frame Relay
ATM

شرح كل من بروتوكول الـ **TCP** و الـ **UDP** :

TCP: Transmission Communication Protocol

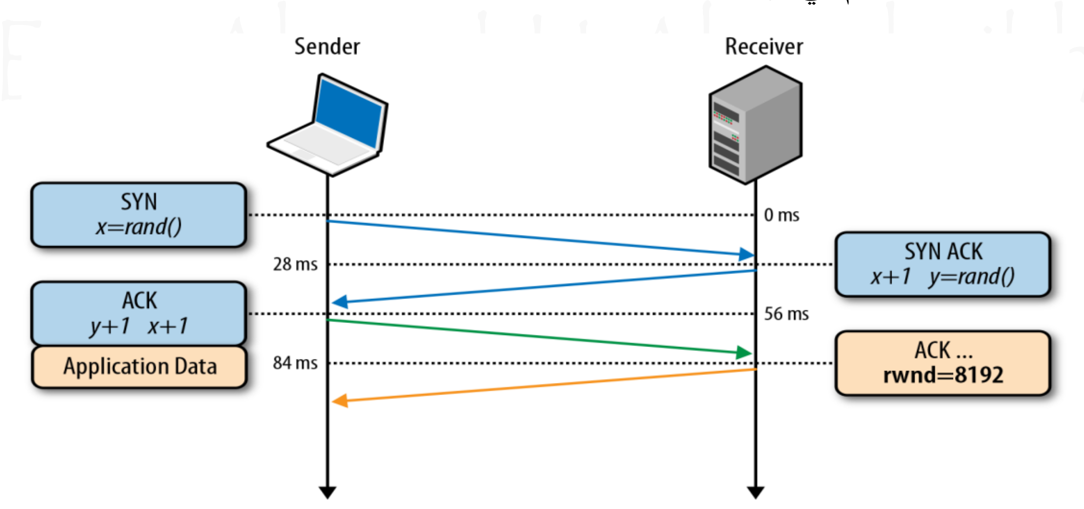
هو بروتوكول يتحقق من وصول البيانات المرسلة و هو يحتاج إلى جلسة عمل ما قبل إرسال البيانات إلى الحاسوب الآخر و تسمى هذه العملية **Three Way handshake** , و من خلال هذه العملية يقوم ببناء جلسة عمل ما بين الجهاز المرسل و المستقبل .

عندما ا يتم إرسال إحدى الرزم من حاسوب إلى آخر فان هذا البروتوكول يتأكد من وصول الرزمة إلى الحاسوب ، و إذا لم تصل فإنه يقوم بإرسال الرزمة مرة أخرى ، حتى يتأكد من أنها وصلت و بعد ذلك يرسل الرزمة الثانية و يتأكد من وصولها و بعد ذلك يرسل الثالثة و هكذا حتى تكتمل كل الرزمة بشكل كامل .

تتم هذه العملية بناءاً على ما يسمى **Connection Based**

حيث أن الحاسبان اللذان يتراسلان البيانات يتفقان على كمية بيانات محددة سوف يتم إرسالها في الوقت واحد و ذلك بناءاً على سرعة الحاسبان و يتم الاتفاق على أمور أخرى و هذا ما يسمى بجلسة العمل .

- هذه الصورة تعبر عن كيفية إرسال و استقبال البيانات ما بين الحواسيب و كيفية بناء الاتصال ما بينهم في بروتوكول الـ **TCP** .



قبل الانتقال إلى بروتوكول الـ **UDP** يجب أن نتعرف على نقطة مهمة جداً جداً جداً جداً :

بروتوكول الـ **UDP** يعتمد على طريقة **Connectionless** بمعنى إنه لا يقوم ببناء الاتصال ما بين المرسل و المستقبل مثل بروتوكول الـ **TCP** بل إنه يرسل رسالة لعنوان المستقبل بشكل مباشر من دون بناء جلسة عمل ما بين الأجهزة و التي تسمى بعملية الـ **Three Way handshake.**

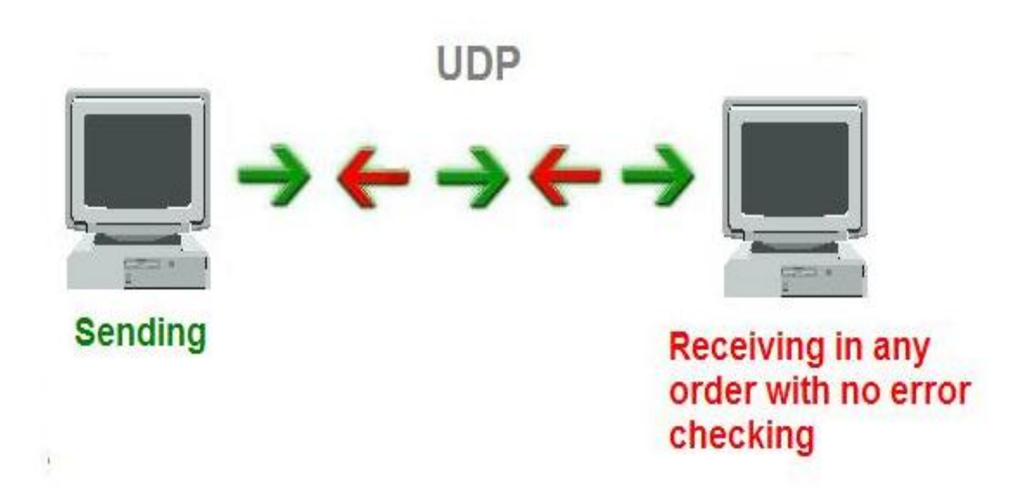
بروتوكول الـ **TCP** يعتمد على طريقة **Connection-Oriented** بمعنى إنه يقوم ببناء اتصال ما بين المرسل و المستقبل ، قبل عملية الإرسال و حيث إنه يقوم ببناء عملية اتصال كاملة و مباشرة ما بين المرسل و المستقبل.

UDP: User Datagram Protocol

بروتوكول بيانات المستخدم يقوم بتقسيم الرسالة إلى عدة أجزاء و يقوم بإرسال هذه الأجزاء إلى المستقبل مع وضع عنوان المستقبل في كل جزء من أجزاء الرسالة طبع ، و يرسل هذه الأجزاء في فضاء الانترنت مما قد يجعل جزء يصل قبل جزء آخر فهذه الأجزاء لا تسلك نفس الطريق في الشبكة.

إن هذا البروتوكول لا يقدم أي ضمان لوصول الحزمة بشكل صحيح أو كامل لان هدف هذا البروتوكول هو إيصال الحزمة بشكل سريع وفي اقرب وقت ممكن، و ليس هدفه إيصال الحزمة بشكل صحيح و التأكد من وصولها بسلامه كما يفعل بروتوكول الـ **TCP**.

- هذه الصورة توضح كيفية إرسال البيانات بشكل مباشر من دون جلسة عمل مسبقة أو بناء عملية اتصال مسبقة على عكس بروتوكول الـ **TCP** .



الفرق بين UDP و TCP :

بروتوكول الـ **UDP** أسرع من بروتوكول الـ **TCP** لان الـ **UDP** لا يتحقق من صحة وصول الرزم بعكس الـ **TCP** الذي يتحقق من صحة و سلامة وصول كل رزمة من البيانات .

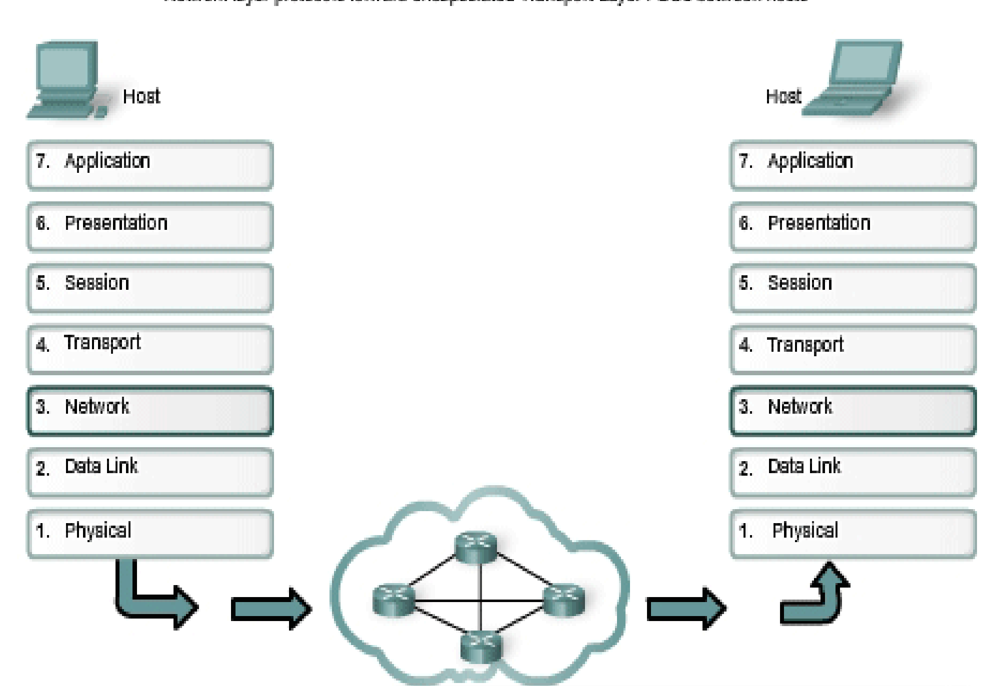
إذا أرسلت حزمتين عن طريق بروتوكول الـ **UDP** فانك لا تعرف أيهما سوف تصل أولاً لان كل واحدة من الحزم تسلك طريقا مختلف ، أما ببروتوكول الـ TCP فان الحزمة تصل بالترتيب حسب ما أرسلها المرسل فالرسالة التي أرسلت أولا تصل أولا و هكذا .

التطبيقات التي تعمل في الـ **TCP** و **UDP** التطبيقات المشتركة مثل البروتوكولات :

FTP = Port 21, Telnet = Port 23, SMTP = Port 25, DNS = Port 53, TFTP = Port 69, SNMP = Port 161, RIP = Port 520.

3- Network layer

هذه الطبقة المختصة في الشبكة و هي المسؤولة عند ادارة الـ **Packet** تتم عملية التحويل إلى Packet بعد نزول الداتا من طبقة النقل **Transport layer** يتم نزول الداتا على شكل **segment** و بعد وصولها لطبقة الشبكة **Network layer** يتم تحويلها من **segment** إلى **Packet** و بعده يتم إضافة **IP** جهاز المرسل و جهاز المستقبل و بعد هذه العملية تقوم هذه الطبقة بتحديد مسار الـ **Packet** الذي سيتم نقل البيانات منه و الذي يسمى الموجه أو التوجيه **routing** في هذه المرحلة يتواجد في المسار بروتوكولات توجيه المستخدمة ما بين الموجهات أو الراوترات مثل بروتوكولات **OSPF** , **EIGRP** , **RIP** و **BGP**.



البروتوكولات التي تعمل في طبقة الشبكة - **Network layer** :

IPv4, IPv6 , IPx , ICMP , IPsec , IGMP,CLNP,EGP,EIGRP,IGRP,IPx

SCCP, GRE, OSPF, ARP, RIP, Routed-SMLT

هذه الطبقة هي المسؤولة عن الشبكة بشكل مباشرة في عملية توجيه البيانات من شبكة لـ شبكة اخرى في منطقة اخرى و هي المسؤولة ايضاً عن عملية الربط ما بين الراوترات أو الموجهات و هذه الطبقة من أهم الطبقات الذي يجب على الدارس فهما جيداً في حال وقوع مشكلة في الشبكة يجب المعرفة في اية طبقة من الطبقات السبعة المشكلة موجودة ليتم حل هذه المشكلة بشكل سريع .

2-data link layer

طبقة ربط البيانات أو طبقة ربط المعطيات طبقة ربط البيانات هي الطبقة التي يتم فيهاتجهيز البيانات من أجل تسليمها للشبكة اي تحويل البت الخام إلى جدول من الإطارات.

و يتم تغليف الحزم (**Packet**) في إطار (**FRAME**) وهو مصطلح يستخدم لوصف حزم البيانات الثنائية (**binary data**) البروتوكولات في هذه الطبقة تساعد في عنونة واكتشاف أخطاء ومعالجة الأخطاء في البيانات التي سترسل وتستقبل. وتقوم بعملية نقل كتل من البيانات عبر الرابط الفيزيائي (المادي). فالحواسيب المضيفة ترسل من وإلى واجهات معالجات الرسال (**Interface Message Processor IMP**) التي تعالج الاتصالات عبر رابط الاتصال المادي.

بشكل عام تكون مهمة طبقة ربط البيانات صنع خط فيزيائي يظهر الخطأ إلى الطبقات الأعلى وهذا ما يدعى بالدارة الافتراضية.

هكذا الطبقة الأعلى من التسلسل الهرمي.

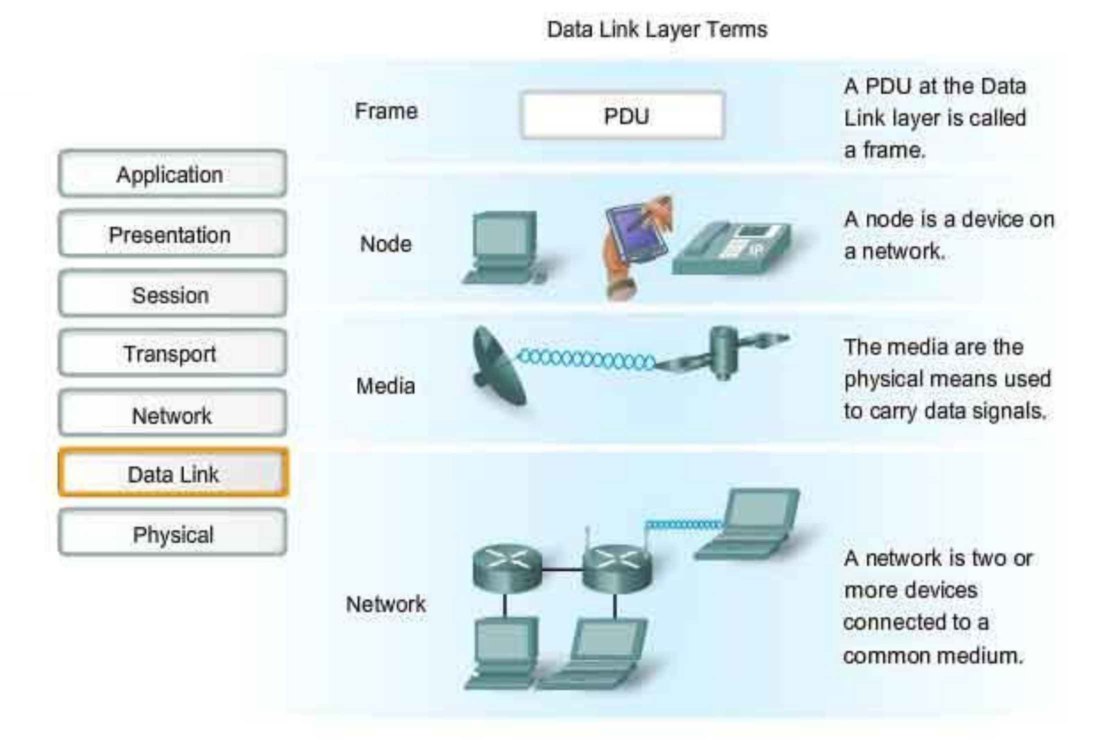
البرتوكولات تستطيع تمرير البيانات إلى الأسفل حيث الطبقات المنخفضة وتكون قادرة أن تفترض إذا كانت الرسالة وصلت إلى وجهتها بالإضافة إلى أنه من المهم أن يحصل المستقبل على البيانات بنفس الشكل المرسل. وهذا مايعرف بشفافية البيانات والتي تعني أن البيانات المنقولة لا تتغير ولا تحرف.

طبقة التحكم بالربط المنطقي :

أو طبقة التحكم المنطقية **Logical Link Control LLC** يتم فيها تحويل ال **Bits** إلى **Bytes** ثم تحويلها إلى **Frames** ويتحدد نوع وحجم ال **Frame** حسب ال **Logical Network Topology** والمقصود بها طريقة تخاطب الأجهزه هل تستخدم ال **Token ring** مثلا أم ال **star** مثلا وهى الطريقة الشائعة فحجم ال **Frame** يختلف هنا وأيضا حسب نوع البروتوكول المستخدم يختلف حجم ال == **Frame** طبقة التحكم بالوصول إلى الوسائط : **Media Access Control MAC** == يتم في هذة المرحلة وضع العنوان ماك **Mac Address** الخاص بكرت الشبكة وهو متفرد ولا يتكرر في أى جهاز إلى ال **Frame** وأيضا بحث طريقة وضع البيانات على الكابل بطريقه لاتتعارض مع وضع جهاز آخر للبيانات على الكابل في نفس الوقت.

المشاكل التي تواجه طبقة ربط البيانات :

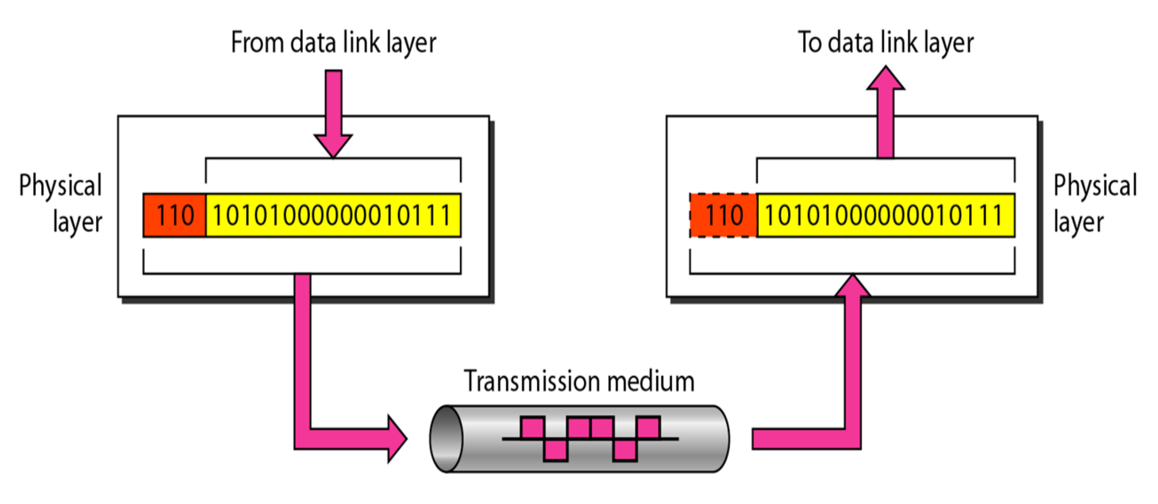
١. أخطاء على الرابط المادي بسبب الضوضاء وأخطاء خط.
٢. معدل نقل البيانات من الخط محدود على النحو الذي يحدده عرض النطاق الترددي.
٣. سرعة تجهيز محدودة من قبل المضيف وواجهات معالجات الرسالة (**IMP**).
فالمضيف يستطيع فقط الموافقة على بيانات ضمن مجال معين.
٤. حجم الذاكرة المؤقت على (**RAM** ذاكرة الوصول العشوائي) .



Data link layer

1-Physical layer

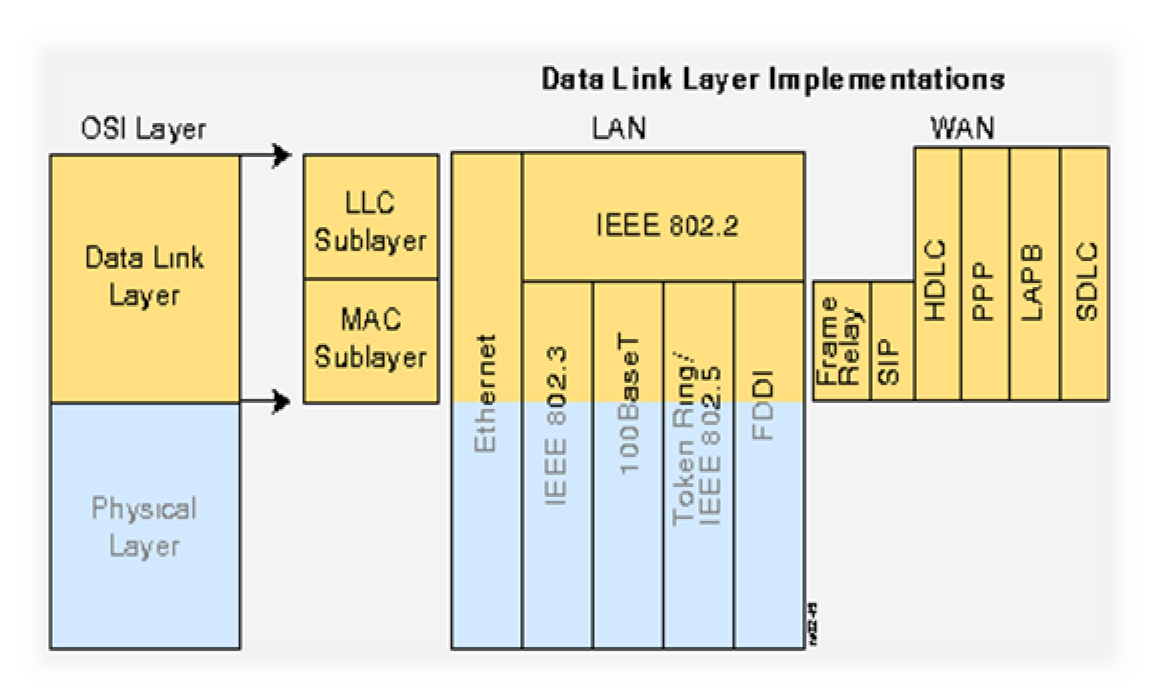
هذه الطبقة الاخيرة من الطبقة السبعة و هي آخر مرحلة تمر فيها البيانات أو الداتا بشكل نهائي ليتم ايصاله للجهاز المطلوب , و في هذه المرحلة يتم تحويل الداتا أو البيانات عند الوصول لهذه الطبقة تكون على شكل فريم **Frame** و تتم عملية التحويل من فريم **Frame** إلى اشارات كهربائية **BITS** و يقوم بهذه الوظيفة كرت الشبكة و المودم و بعد الانتهاء من هذه العملية يستم التسليم لكابل الشبكة المتوصل في كرت الشبكة و بعده ستبحر البيانات في عالم الشبكة للوصول إلى الجهاز المطلوب .



Physical layer

البروتوكولات التي تعمل في طبقة ربط البيانات و الطبقة الفزيائية

Data link layer - Physical layer



- الأن لنتعرف على شكل الداتا في كل طبقة من الطبقات السبعة في الجدول التالي :

Application layer	Data
Presentation layer	Data
Session layer	Data
Transport layer	Segment
Network layer	Packet
Data link layer	Frame
Physical layer	Bites

- الأن لنتعرف على الأجهزة التي تعمل في كل طبقة من الطبقات السبعة في الجدول التالي :

Application layer	PC
Presentation layer	PC
Session layer	PC
Transport layer	Switch Core
Network layer	Router
Data link layer	Switch , HUB
Physical layer	NIC, Cable

الأن ناتي للتوضيح الاكثر أهمية في الحياة الحقيقة و العملية كل هذا الشرح هو عبارة عن شرح و مفهوم للطبقة السابعة **OSI Layers** ولا يوجد له وجود ولكن في الحياة الحقيقة يوجد ما يسمى الـ **TCP/IP** و هو مكون من اربعة طبقات ماخوذ من النموذج الأول و هذه الصورة توضح نموذج الـ **TCP/IP** .

OSI Model	TCP / IP
Application	Application
Presentation	
Session	
Transport	Transport
Network	Internetwork
Data Link	Link and Physical
Physical	

الأن بعد أن فهمت النموذج الأول و هو النموذج المكون من السبع طبقة الأن يسهل عليك فهم النموذج الثاني و هو الـ **TCP/IP**.

TCP/IP

Transmission Control Protocol / Internet Protocol

لقد تم اختراعها سنة 1970، وكانت جزء من أبحاث مؤسسة

DARPA ، التي قامت لتوصيل أنواع مختلفة من الشبكات وأجهزة الكمبيوتر. وكان تمويل هذه المؤسسة عاما من أجل تطوير هذه" اللغة"، ولذلك فإنها تتصف بعدم تبعيتها لأحد ، والنتيجة أنها أصبحت ملكا عاما، وبالتالي لا يمكن لأحد ادعاء الحق باستخدامها له فقط.

واكثر من هذا فان بروتوكولات **TCP/IP** تتكون من عتاد **Hardware** وبرامج **Software** مستقلة ، ولذلك فان اى شخص يمكن له أن يكون متصلا بالانترنت ويشارك فى المعلومات مستخدما اى نوع من أجهزة الكمبيوتر.

ماهوالبروتوكول:

البروتوكول بالنسبة للكمبيوتر على الإنترنت عبارة عن مجموعة القواعد التي تحدد كيف يمكن لأجهزة الكمبيوتر أن تتفاهم مع بعضها البعض عبر الشبكة التي تتواجد عليها. وشبكة الكمبيوتر تعني جهازي كمبيوتر أو أكثر متصلة مع بعضها البعض وقادرة على أن تتشارك في المعلومات . عندما ا تتحادث أجهزة الكمبيوتر مع بعضها البعض فإن ذلك يعني تبادلها مجموعة من الرسائل. وحتى يكون في إمكانها فهم تلك الرسائل والعمل على تنفيذها

فإن على أجهزة الكمبيوتر الموافقة على العمل بقواعد واحدة متفق عليها. فإرسال واستقبال البريد الإلكتروني ونقل الملفات والمعلومات وغيرها هي أمثلة على ما تقوم به أجهزة الكمبيوتر عبر الشبكات باستخدام مجموعة القواعد التي تحدد طريقة تفاهم أجهزة الكمبيوتر مع بعضها أو ما أسميناه بالبروتوكول.

إن البروتوكول يقوم بوصف الطريقة التي يجب على تلك الأجهزة أن تتبادل فيها الرسائل وتنتقل المعلومات.
البروتوكول يختلف باختلاف نوع الخدمة التي تقدمها الشبكة ، وعلى سبيل المثال فإن الإنترنت قد تأسس على مجموعة البروتوكولات التي تكون عائلة واحدة هي **TCP/IP**

TCP/IP في الواقع هو عبارة عن بروتوكولين مختلفين ولكنهما يعملان معا دوما في نظام الإنترنت، ولهذا السبب فإنهما أصبحا مقبولين لأن يوصفا بأنهما وكأنهما نظام واحد.

إن بروتوكول **TCP/IP** في الواقع يعتمد عليه جميع أساليب العمل خلال الإنترنت وأنه على أسس هذا البرتوكول تأسست بروتوكولات تكون عائلة واحدة من خلال بروتوكول **TCP/IP** ، ومن أهم هذه البروتوكولات :

Simple Mail Transfer Protocol (SMTP) ويتحكم في طريقة إرسال واستقبال البريد الإلكتروني .

File Transfer Protocol (FTP) وذلك لنقل الملفات بين أجهزة الكمبيوتر .

Hypertext Transfer Protocol وذلك لبث أو إرسال المعلومات على صفحات الشبكة العالمية **World Wide Web (www)**

إن هذه البروتوكولات تستطيع تمكين الأنواع المختلفة من أجهزة الكمبيوتر مثل الكمبيوتر الشخصي **PC** وماكنتوش ولينيكس وغيرها من أن تتفاهم مع بعضها على الرغم من اختلافاتها، والسبب هو أن تلك البروتوكولات تستعمل تركيبة معيارية واحدة في عملية التفاهم .ما هو السيرفر ؟ السيرفر هو عبارة عن جهاز كمبيوتر يتم تشغيل أحد الانظمةالتالية على **Linux** و الذي يستخدم كمنصة لإطلاق تطبيقات الويب المفتوحة المصدر (**php**) أو ويندوز و الذي يستخدم لإطلاق تطبيقات الويب الخاصة بمايكروسوفت و المعروفة بـ (**ASP**) أي و بشكل مختصر تحول تلك الملفات البرمجية إلى مواقع ويب قابلة للعرض من أي مكان في العالم و تصبح بصيغة (**HTML**) .

حزمة أنظمة الإنترنت هي بنية تصميمية تحدد مجموعة من الأنظمة المستخدمة للاتصال في الشبكات الحاسوبية. تقوم عليها شبكة الإنترنت العالمية حيث تؤمن التوافقية في ارتباط الشبكات المختلفة في أرجاء العالم مع بعضها البعض. وهي عبارة مجموعة بروتوكولات مرتبطة مع بعضها وتعمل معا.

تسمى أحيانا بحزمة النظم **TCP/IP** اختصار لـ **Transmission Control Protocol/Internet Protocol** نسبة لبروتوكول **TCP** وبروتوكول أوائل البروتوكولات التي ظهرت.

للحزمة ما يقابلها في نظام **OSI** الفرق بين الإثنين يكمن في كون الأولى اخترعت لحل مشكلة واقعية في الاتصالات، أما **OSI** فهو نظري أكثر منه تطبيقي.

وكغيره من بروتوكولات الاتصال، فإن **TCP/IP** مؤلف من طبقات: طبقة الـ **IP** هي المسؤولة عن نقل حزم البيانات من حاسب لآخر، حيث يقوم بروتوكول **IP** بإرسال كل رزمة بناءً على عنوان وجهة المعطيات المؤلف من أربعة بايتات، أو مايعرف برقم **IP**. وتقوم الهيئات المسؤولة عن الإنترنت بتعيين مجالات من هذه الأرقام لمختلف الشركات، وتقوم هذه الشركات بتعيين مجموعة من أرقامها لمختلف الأقسام.

المداخل SOCKETS : هي عبارة عن تطبيقات جزئية مسؤولة عن السماح بالدخول إلى معظم الأنظمة من خلال بروتوكول**TCP/IP** ، الذي لايستخدم فقط للدخول إلى الانترنيت، وإنما يستخدم أيضاً على نطاق واسع لبناء الشبكات الخاصة. وقد تكون هذه الشبكات الخاصة مرتبطة بالانترنيت، وقد لا تكون مرتبطة بأي شبكة أخرى. ونسمي الشبكة الخاصة التي تستخدم بروتوكول **TCP/IP** وبرمجيات الانترنيت، بشبكات انترنيت.

وتحتوى كل طبقة على مجموعة من القواعد والبوتوكولات التي تقدمها للطبقات التي تليها ومن الجدير بالذكر انك لاتشعر بأى طبقة من تلك الطبقات، أنت فقط تشعر بالطبقة الأخيرة وهي طبقة البرامج وهي التي تستخدمها البرامج المعروفة مثل المتصفحات وقارئ البريد الاكتروني أو برامج المسنجر.

بروتوكول التحكم بالإرسال بروتوكول الإنترنت (TCP/IP) :

Transport Control Protocol / Internet Protocol إذا كان لدينا عنوان اي بي فذلك يعني أن لدينا بروتوكول **TCP/IP** فعند تثبيت هذا البروتوكول يجب أن نعرف رقم اي بي واحد على الأقل في الشبكة ثم نعين مخدم **DHCP** يوزع الأرقام على جميع الحواسيب، ويمكن أن نلخص مفهوم **IP**على النحو الاتي رقم **IP** هو لتعريف الجهاز في الشبكة (موقع وجوده أو ربطه الفيزيائي على الشبكة) وهو يشبه كثيرا رقم الهاتف فكل جهاز يدخل إلى الشبكة يكون له رقم متفرد خاص لا يملكه جهاز أخر ومثلا شبكة الأنترنت في وقت واحد لا يكون في العالم كله رقمين متشابهين وفي شبكة خاصة لو تعين رقمين متشابهين لن يستطيعوا الاتصال في ما بينهم يتألف عنوان **IP** الإصدار الرابع من **32** بت مقسمة ألى اربع مجموعات وكل مجموعة تحتوي على **8** بت وتمثل هذه البتات بأرقام عشرية مثل **131,107,2,200** وبما أن كل مجموعة مكونه من **8** بت فيمكن أن يكون أي مجموعة من الرقم **1** ألى **255** بالنظام العشري أو ثماني خانات (بت) بالنظام الثنائي

يتم تقسيم البروتوكولات الحزمة TCP/IP :

طبقة التطبيقات	**Application**
طبقة النقل	**Transport**
طبقة الإنترنت	**Internet**
طبقة الربط	**Network Interface**

أجهزة الشبكة

Network Devices

أجهزة الشبكات بشكل عام و شرح كل نوع بالتفصيل مع ذكر امثلة على كل جهاز :

١- **الموزع HUB :** هو أحد أجهزة الشبكة و من أهم الأجهزة التي يجب أن تكون في داخل الشبكة هذه يقوم بعمل اكثر من وظيفة في نفس الوقت , يقوم بربط مجموعة من أجهزة الحاسوب لي يتمكنو من العمل في نطاق واحد و شبكة واحدة يتم ربط كل جهاز حاسوب في منفذ من منافذ الهاب .

- كيفية عمل جهاز الهاب يقوم أحد أجهزة الكمبيوتر بإرسال بيانات إلى أجهزة اخرى على نفس الهاب تصل هذه الرسالة إلى الهاب و يقوم الهاب باخذ هذه الرسالة و نقلها إلى جميع المنافذه المتصله فيه أجهزة الحاسوب و سوفه تتلقى جميع الأجهزة هذه الرسالة مما يعمل ثقل و اختناق في الشبكة و عند الوصول للجهاز المطلوب سيتم اخذها و عمل حذف للرسالة عن باقي الأجهزة التي تم الوصول اليهم هذه الرسالة .
- يقوم جهاز الهاب بتكرار الإشارة مثل جهاز المكرر الذي سنقوم بشرحه لاحقاً .
- يعمل جهاز الهاب في الطبقة الأولى **Physical Layer** ويفهم فقط الإشارة الكهربائية.

- يوجد عدة أنواع من جهاز الهاب **HUB** .

١- **Passive Hub** الهاب الذي يكون مفعل فيه الكهرباء من غير كابل كهرباء.
٢- **Active Hub** الهاب الذي ياتي معه كابل كهرباء و يكون له مقبس كهرباء.
٣- **Hybrid Hub** الهاب الهاجين الذي يقوم بربط أكثر من هاب على مختلف انواعه.
٤- **Smart (intelligent) Hub** الهاب الذكي.

صورة الهاب



٢- **المبدل Switch :** يعمل المبدل أو الموزع على ربط أجهزة الحاسوب ببعضها البعض على الشبكة ليتم العمل في نطاق واحد و شكبة واحدة و فكرة عمله مشابه لجهاز الهاب و الجسر **Bridge** حيث أن كلاهما يعملان في نفس الطبقة الأولى **Physical Layer** و الطبقة الثانية **Data Link Layer** في طبقة الـ **OSI** يتميز هذا الجهاز بسرعة اداه و افضل من جهاز الهاب لان فكرة عمله نفس فكرة عمل الهاب ولكن المبدل أو الموزع **Switch** أفضل منه في نقاط معينة مثل تقسيم مجال التصادم و جدولة العناوين الفيزيائية و فائدة هذا الجدول تنظيم الإرسال و تسجيل الماك ادرس الخاص بكل جهاز حاسوب متصل في المبدل على عكس الهاب لا يوجد فيه جدول العناوين ولا يفهم عناوين الأجهزة وكل الهاب يعتبر مجال تصادم واحد .

- **المميزات التي توجد في المبدل Switch ولا توجد في الهاب Hub :**

١- المبدل يحتوي على جدول العناوين الفيزيائية و يقوم بتسجيل الماك ادرس في الجدول بعد التعرف على جميع أجهزة الحاسوب التي تم توصيلها في المبدل بعد هذه العملية عندما يريد جهاز حاسوب متصل على منفذ رقم **8** يريد إرسال بيانات لجهاز حاسوب متصل على منفذ **5** عنده سيقوم السويتش بعمل التالي ياخذ البيانات و يقوم بنظر على جدول العناوين الفيزيائية ينظر على عنوان الجهاز المطلوب و يقوم بإرسال البيانات اليه بعينه من دون أن يقوم بإرسال البيانات لكل المنافذ الموجودة على السويتش .

- كيف تتم عملية الإرسال بشكل مباشر و عدم إرسال البيانات لكل المنافذ على السويتش ؟

يوجد في داخل السويتش جدول يقوم بتسجيل جميع الـ **Mac-Address** الخاص في أجهزة الحاسوب و بهذه الطريقة عندما يريد جهاز معين إرسال بيانات لجهاز معين سيقوم الجهاز الذي يرد إرسال البيانات بتغليف الـ **Frame** مع الـ **Mac-Address** بعد هذا سيتم وصول الـ **Frame** للسويتش و عمل البث المباشر **Broadcast** على السويتش لمعرفة الماك ادرس الذي ياخذ رقم المنفذ و يتم الإرسال اليه مباشرة .

٢- السويتش يعمل بصيغة (**One – to – One**) .

٣- يقوم بتقسيم مجال التصادم **Collision Domain**.

٤- يعمل في الطبقة الأولى و الثانية من بقطة الـ **OSI**.

٥- يوجد في داخله **Mac-Address-Table** لتسجيل العناوين .

٦- لا يفهم الاي بي فقط يفهم الـ **Mac-Address**.

٧- عنوان البث المباشر لجهاز السويتش **ffff.ffff.ffff**.

٨- كل منفذ يعمل بسرعته ولا يشترك في سرعة المنافذ مثل الهاب .

صورة السويتش



٣- **المكرر Repeater :** يعد هذا الجهاز من الأجهزة المهمة جداً في الشبكة هذا الجهاز يقوم بتكرار الإشارة و يعمل في الطبقة الأولى و هي الطبقة الفيزيائية و هذا الجهاز هو من ابسط أنواع أجهزة الشبكة و يقتصر عملها على تكرار الإشارة فقط كل ما يتم الوصول لحد إنهاء الإشارة يقوم جهاز المكرار بتجديد الإشارة و اعادة إرساله من جديد .

- يتم أستخدام المكرار عندما نريد توصيل مسافة أكبر من المسافة التي يدعهما كابل الـ **Twisted pair** هذا الكابل فقط يدعم لحد **٩٠ متر** و بعده سيتم التقطع في البيانات و عدم وصول البيانات بشكل سليم عنده سياتي حاجت المكرر نقوم بتركيب المكرر على آخر نقطة في الكابل و نقوم بتوصيل كابل آخر و بهذه الطريقة سيتم التوصيل لمسافة ابعد من **٩٠ متر** بشكل سليم و عدم التقطع في الإشارة أو البيانات .

صورة المكرر



٤- **الموجه Router :** الموجه يعتبر من أهم الأجهزة المستخدمة في ربط الشبكات المختلفة الكبيرة و البعيدة و القريبة و يعمل في الطبقة الثلاثة **Newtork Layer** .

- **الموجه يقوم بعمل أكثر من وظيفة :**

١- يقوم بربط الشبكات المختلفة عن بعض مثل يوجد شبكة بعنوان **10.0.0.0** و شبكة بعنوان **192.168.1.0** الأن يوجد شبكتان نريد ربط ما بين هذه الشبكات ليتم التوصيل ما بينهم في هذه الحال نحتاج الموجه أو الراوتر ليقوم بربط هذه الشبكات و التوصيل ما بينهم .

٢- يقوم بتحديد و اختيار افضل مسار من اصل مجموعة مسارات لتتم عملية إرسال و استقبال البيانات من المرسل **Source** إلى المستقبل **Destination** أو العكس من خلال هذا المسار و يستخدم ايضاً لعملية الربط على شبكة الانترنت .

ملاحظة : الراوتر لا يعني المودم الـ **ADSL** الموجود في المنزل الموجود في المنزل هو عبارة عن مودم **ADSL** وليسه راوتر أو موجه .

صورة الموجه - Router



صورة المودم - Modem



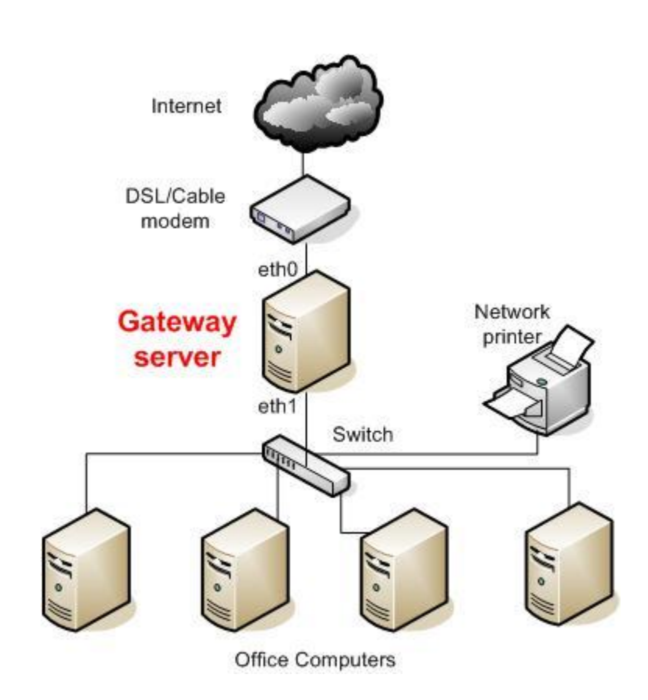
٥- **جهاز البوابة Gateway :** يعتبر هذا الجهاز من اذكى أجهزة الشبكة و يعمل في جميع مستويات الـ **OSI** في البطقة السبعة و هو جهاز لا يعرفه الكثير من الاشخاص ولكنه مهم جداً جداً و هو جهاز بأختصار يقوم بربط شبكتين مختلفة كلياً عن بعض حيث يقوم بعمل ترجمة أو وسيط بين الشبكتين و في الواقع فهو يعبر عن جهاز الموجه **Router** ولكن في جهاز الراوتر تم إضافة جهاز الـ **Gateway** ليتم العمل في داخل الراوتر بشكل أفضل .

- **ينقسم جهاز الـ Gateway إلى قسمين :**

١- **External Gateway** : و هذا النوع يربط ما بين الشبكات المختلفة كلياً في البينة التحتية مثل ربط شبكة حاسوب بشبكة جوال .
٢- **Internal Gateway** : و هذا النوع يستخدم بربط شبكتين في نفس المبنى على مختلف الشبكات مثل شبكة تختلف عن الآخر من ناحية الاي بي و نقوم بربطهم بهذا النوع من الـ **Gateway** ليتم التوصيل بينهم.

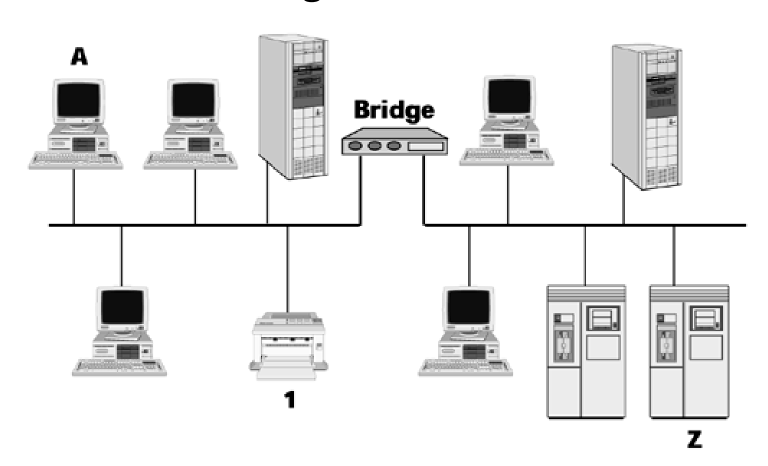
صورة جهاز الـ Gateway





٦- **جهاز الجسر Bridge :** يعمل هذا الجهاز على ربط شبكتين **LAN** ببعضهما البعض بحيث يعملان في شبكة واحدة و ينشئ هذا الجهاز جدول توجيه **Routing Table** يتضمن العناوين الفعلية للأجهزة و يحدد هذا الجدول الواجهة الرئيسية للرسالة .

صورة الجسر – Bridge



٧- **كرت الشبكة NIC :** كرت الشبكة و هو عبارة عن كرت الغرض منه نقل و استقبال البيانات من و إلى الـ **NIC** و تتم هذه العملية من خلال جهاز إرسال و استقبال الإشارة (**Transceiver**) في الـ **NIC** و أهم شياء يجب معرفته عن الـ **NIC** هو إنه يحتوي على الـ **MAC Address** و كل كرت يختلف عن الآخر ولا يمكن تكرار الماك ادرس على اكثر من كرت .

NIC = Network Interface Card



١- يعمل في الطبقة الأولى و الثانية من طبقة الـ **OSI** .
٢- يخزن البيانات قبل معالجتها و إرسالها .
٣- يتم التاكد من خلو الكابل الخاص في الشبكة قبل الإرسال عن طريق الالية يستخدمه كل من أنواع تقنيات الشبكة المحلية في الإيثرنيت يتم استخدام الالية الـ**CSMA/CD**.
٤- يقوم بتغليف البيانات بوضعها في داخل إطار و وضع عنوان المرسل و المرسل اليه.

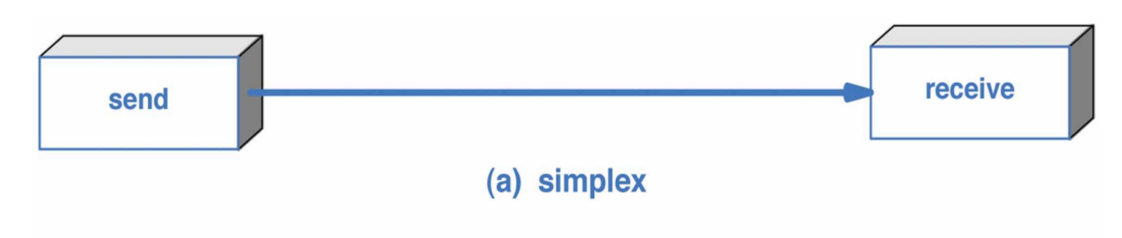
طرق إرسال البيانات في الوسط المادي للشبكات

Methods of Sending Data in the Physical Media Networks

- يوجد أكثر من طريقة لعلمية إرسال البيانات في أجهزة الشبكة أو الوسط المادي على مختلف أنواع الأجهزة التي سيتم ذكره في الشرح .

Simplex

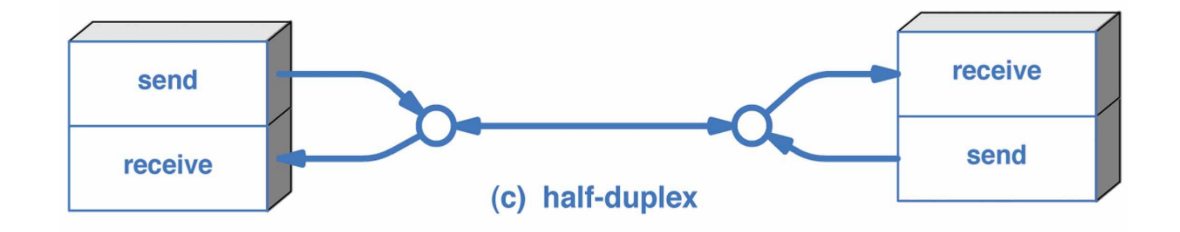
الإرسال في اتجاه واحد من غير القدرة على الرد



(a) simplex

Half Duplex

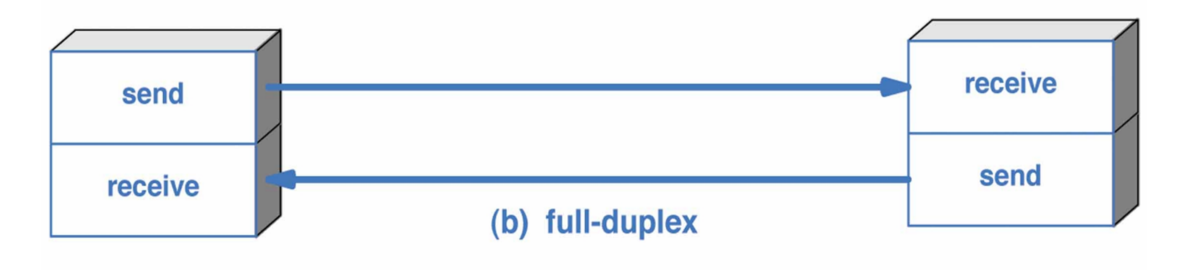
الإرسال نصف المزدوج بشكل متقطع



(c) half-duplex

Full Duplex

الإرسال و الاستقبال في نفس الوقت من دون انتظار



(b) full-duplex

(Simplex)

يوفر نظام الإرسال في اتجاه واحد الإرسال فقط من دون الاستقال أو الرد على المرسل مثل الراديو و التلفزيون .

(Half Duplex)

يوفر نظام الازدواج النصفي عملية اتصال في كلا الجانبين ، لكن بالسماح باتجاه واحد في وقت ما غير لحظي، أي أن الاتجاه الآخر يتم في وقت آخر.

عموماً، عندما ا يبدأ أحد الأطراف باستقبال إشارة ما، فإنه يبقى منتظراً حتى يتوقف المرسل عن عملية الإرسال، قبل الرد.

يعد جهاز ووكي توكي أو الضغط للتحدث أحد أبرز الأمثلة على هذا النوع ، فعملية الاتصال ممكنة بين الطرفين إلّا أنه في الوقت الذي يتحدث فيه أحدهما ينبغي للآخر الاستماع حتى الانتهاء بتحرير زر الاتصال وبالتالي يمكن للأخير ضغط زر الاتصال لبدء دوره وذلك لأن كلا الطرفين يبثاه عبر تردد واحد.

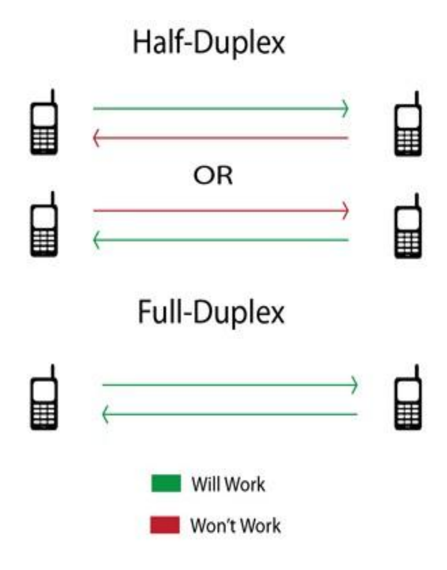
(Full Duplex)

يسمح نظام الازدواج الكامل بالتواصل في كلا الاتجاهين وفي نفس الوقت ، على العكس من الازدواج النصفي.

تمثل خطوط الهاتف المحلية و الهاتف النقال أمثلة على هذا النوع من الاتصالات.

في الحاسوب يمكن أيضاً القول بأن الإيثرنيت تعمل بنفس المبدأ.

لكي تتم عملية الاتصال بالازدواج الكامل ينبغي أن يكون هناك اختلاف مميز بين الطرفين مثل استعمال ترددين مختلفين لمنع تداخل الإشارات أو باستعمال مدأولة ذات تقسيم زمني بمعنى أن يتم إرسال عينات من إشارة كل طرف على فترات زمنية قصيرة غير ملحوظة للأذن البشرية بحيث يمكن إرسالها بشكل متعاقب ومن ثم إعادة فرزها حسب الوجهة.



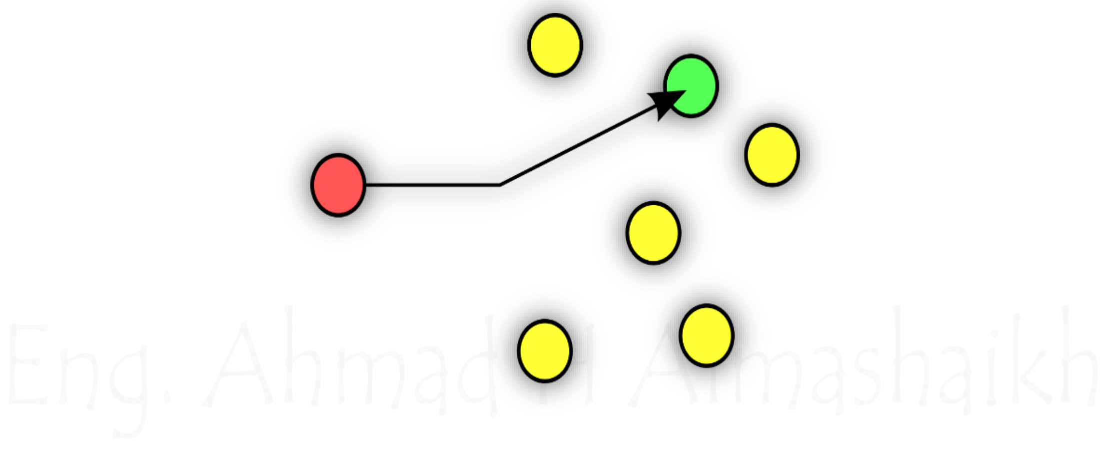
طرق إرسال البيانات في داخل الشبكات

Methods of Sending Data in the Network

طرق إرسال البيانات في داخل الشبكة و يوجد اربع طرق و تم إضافة الطريقة الجديدة بما تمسى **Any Cast** و التي تعمل مع **IPv6** سأقوم بشرح كل واحدة مع ذكر بعض الامثلة على ذالك .

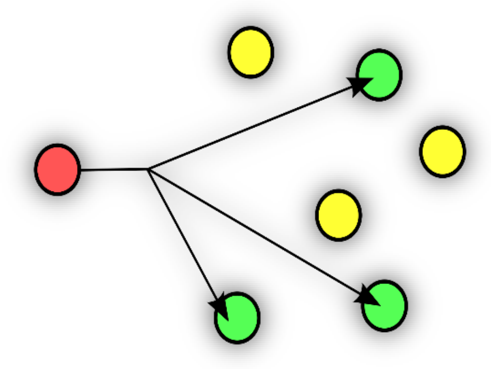
Unicast

هذه العملية تقوم باخذ البيانات و إرساله بشكل موحد للجهاز المطلوب فقط لا غير ولا تقوم بإرسال البيانات لجهاز آخر بمعنى إنه تقوم بعملية الإرسال في اتجاه واحد فقط .



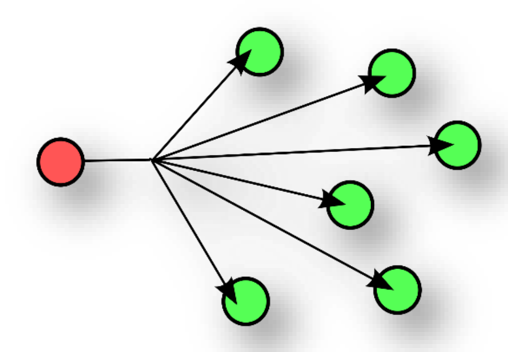
Multicast

الإرسال لمجموعة محددة مثل نقوم بتحديد مجموعة معينه و نقوم بإرسال البيانات لهذه المجموعة فقط مثل لو كان لدينا ٥٠ جهاز و نريد الإرسال لـ ٢٥ جهاز هذه هي المجموعة التي تم تحديده و ستصل البيانات فقط للمجموعة المحددة فقط .



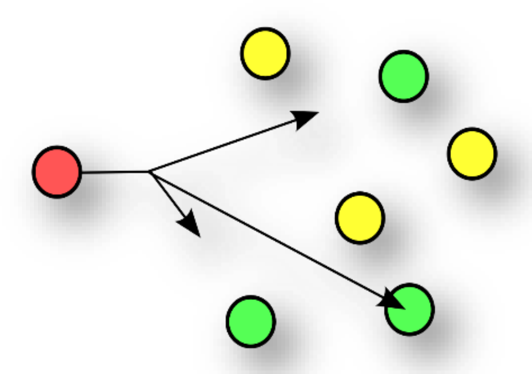
Broadcast

إرسال البيانات لكل الشبكة لجميع الأجهزة المتصلة في الشبكة و هذه العملية تقوم بعمل ثقل في الشبكة و ضغط كبير على الشبكة مما ينتج عن اختاق و حدوث مشاكل في الشبكة .



Any cast

هذه الية لنقل البيانات في الشبكة على شكل اقرب نقطة مثل عندما يتواجد سيرفران أو خادمين من نفس النوع على سبيل المثال خادم ملفات يتكون من خادمين وعندما يرد أحد المستخدمين الوصول لي أحد الخوادم تقوم هذه العملية بفحص اقرب نقطة للوصول و يتم الربط فيها و هذه التقنية افضل بكثير من تقنية الـ **Broadcast** مع العلم إنه تم حذف الـ **Broadcast**من الـ **IPv6** و تم عمل الية الـ **Any cast** .



- **مميزات الـ Any cast :** يوجد عدة مميزات تم وضعها مع هذه التقنية الجديدة :

١- الاعتماد عليه في الشبكة عند وجود اكثر من خادم يقوم بنفس الخدمة.

٢- الامان اصبح اقوى بكثير من ما سبق مثل عندما يحصل هجوم الـ **DDOS** على السيرفرات سيتم توقف السيرفرات ، ولكن مع هذه التقنية اصبح الأمر اصعب .

٣- القدرة على توزيع الترافيك ما بين السيرفرات عند إرسال و استقبال بيانات .

٤- تجنب المشاكل مثل عند حدوث توقف لسيرفر معين و يوجد سيرفر ثاني يعمل بنفس الخدمة سيتم الانتقال عليه من دون أن يعلم المستخدم إنه تم توقف أحد السيرفرات.

مجال تصادم البيانات

Collision Domain

مجال تصادم البيانات : هو عبارة عن التصادمات التي تحدث في داخل الشبكة مما ينتج عن اختناق في داخل الشبكة , و التصادمات يحدث ما بين حزم البيانات في شبكة الـ إيثرنت و يحدث التصادم عندما يقوم أكثر من جهاز على نفس الشبكة المحلية بإرسال حزم من بيانات و في نفس الوقت جهاز آخر يقوم بإرسال حزم من البيانات في هذه الحال ينتج التصادم أو حدوث اختناق في الشبكة .

- يحدث الاختناق عندما نقوم بستخدام جهاز **Hub** أو مكرر الإشارة **Repetar** في الشبكة المحلية **LAN** و يتم حل هذه المشكلة بأستخدام الموزع **Switch** أو الموجه **Router** حيث إنها يقوم بتقسيم مجال التصادم.
- **مع ملاحظة مهم جداً :** الراوتر أو الموجه يقوم بكسر مجال التصادم و يقوم بتقسيم مجال البث ايضاً ويمكن حل مشكلة الاختناق بأستخدام خوارزمية تسمى ناقل متعدد الوصول مع تحسسى التصادم .

- **تحسس الناقل متعدد الوصول مع تحسس التصادم :** قبل قيام اي جهاز بإرسال البيانات، يجب أن يقوم بتحسس الناقل والتأكد من عدم وجود بيانات على ذلك الناقل، عندها يقوم بإرسال البيانات إلى وجهتها.

معلومات مهما جداً جداً :

- الراوتر **Router** : كل انترفيس في الراوتر يعتر مجال بث مباشر **Broadcast** و في نفس الوقت كل انترفيس يعتبر **Collision Domain** .

- السويتش **Switch** : كل انترفيس يعتبر و يعتبر **Collision Domain** , يعتبر **Broadcast**.

- الهاب **Hub** : الهاب يعتبر **Broadcast** و يعتبر ايضاً **Collision Domain**.

الفرق ما بين الـ **Broadcast Domain** و **Collision Domain** :

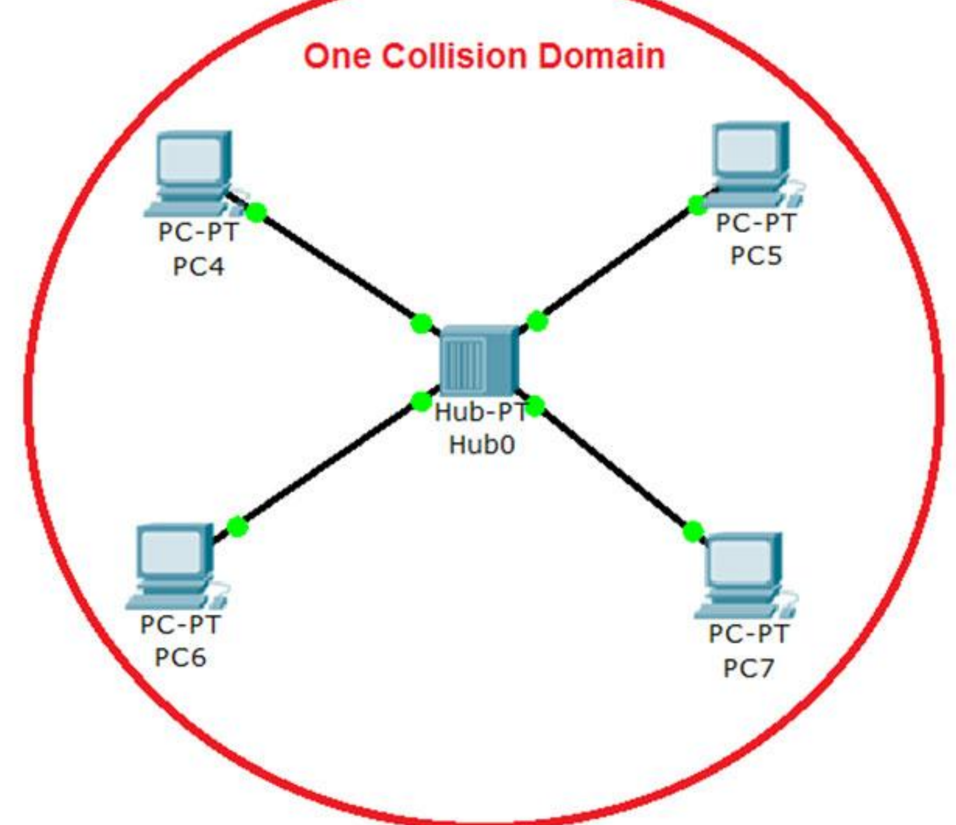
Broadcast Domain : هو عبارة عن مجموعة أجهزة متصلة في شبكة اوحدة تحت نطاق واحد و تحت فئة واحد من عناوين الـ **IP** و تكون نهاية الـ **Broadcast Domain** عند اخرى نقطة للوصول لجهاز الراوتر .

Collision Domain : هو عبارة عن التصادمات التي تحصل عندما تلتقي البيانات في مسار واحد مما يجعل الشبكة تختنق .

- نموذج يعرض فيه جهاز الهاب **HUB** و كما ذكرنا من قبل جهاز الهاب يعتبر كل الجهاز **One Collision Domain** بمعنى كل الجهاز مجال تصادم واحد مما ينتج عن حدوث اختناق في الشبكة و ينتج ثقل و بطء في داخل الشبكة بسبب إرسال اكثر من جهاز في نفس الوقت حزم من البيانات مما يجعل جهاز الهاب غير قادر على تنسيق و معالجة الحزم التي تم إرسالها مره واحد من اكثر من جهاز في نفس الوقت , و ايضاً يعتبر مجال بث مباشر واحد على كل الجهاز مثل عندما ا جهاز ٥ يريد إرسال بيانات لجهاز ٦ سيقوم جهاز ٥ بإرسال البيانات إلى جهاز الهاب سيقوم الهاب ببث هذه البيانات على جميع الأجهزة الموجودة بمعنى سيقوم بإرسال البيانات المرسلة من جهاز ٥ إلى جهاز ٤ و ٦ و ٧ في هذه الحالة سيتم إرسال البيانات لجميع الأجهزة المتصلة في جهاز الهاب و سيقوم كل من الأجهزة بالغاء هذه البيانات و فقط سيتم الموافقة على البيانات من قبل الجهاز المطلوب ٦ فقط , مع العلم جهاز الهاب لا يفهم (**IP**) فقط يفهم اشارة كهربائية و شكل البث المباشر **Broadcast** سيكون كتالي **ffff.ffff.ffff** , و ايضاً لا يدعم الماك ادرس - **Mac Address** .

في هذا النموذج يوجد مجال بث مباشر واحد , و مجال تصادم واحد .

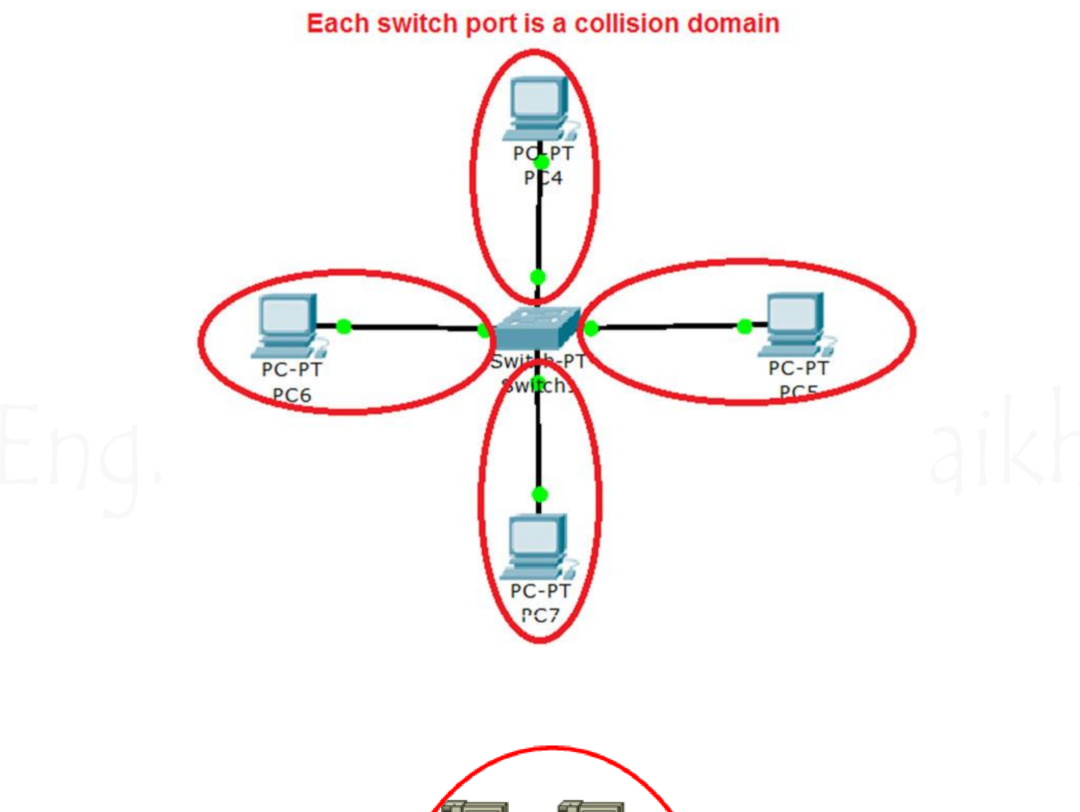
- Broadcast Domain 1
- Collision Domain 1

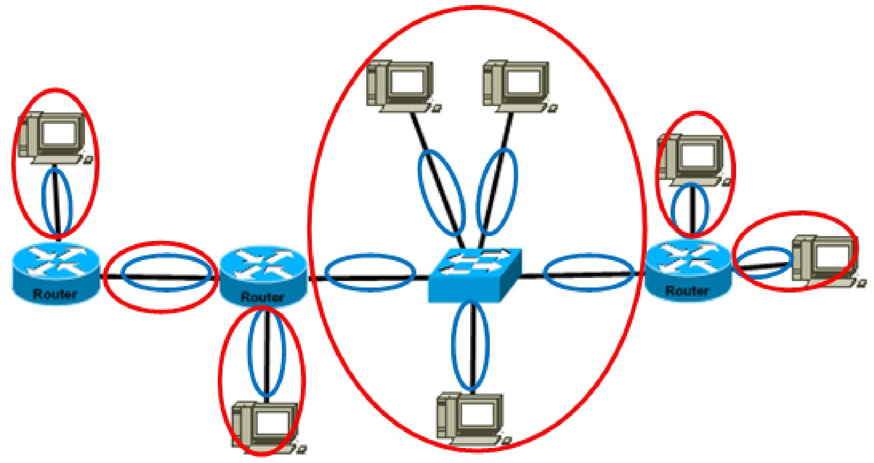


- نموذج يعرض فيه جهاز السويتش و يوجد في هذه النموذج سويتش واحد , ولكن كل انترفيس في السويتش مقسم مجال تصادم واحد كما هو موضح في الصورة التالية و كل انترفيس ياخذ سرعته لوحده على عكس الهاب الذي يشترك في سرعة جميع الإنترفيس و السويتش يفهم العناوين الفزيائية الماك ادرس **Mac Address** , و السويتش كله **Broadcast** بث مباشر على جميع الإنترفيس المركبة على السويتش .

في هذا النموذج يوجد مجال بث مباشر واحد , و يوجد اربعة مجالة تصادم .

- Broadcast Domain **1**
- Collision Domain **4**

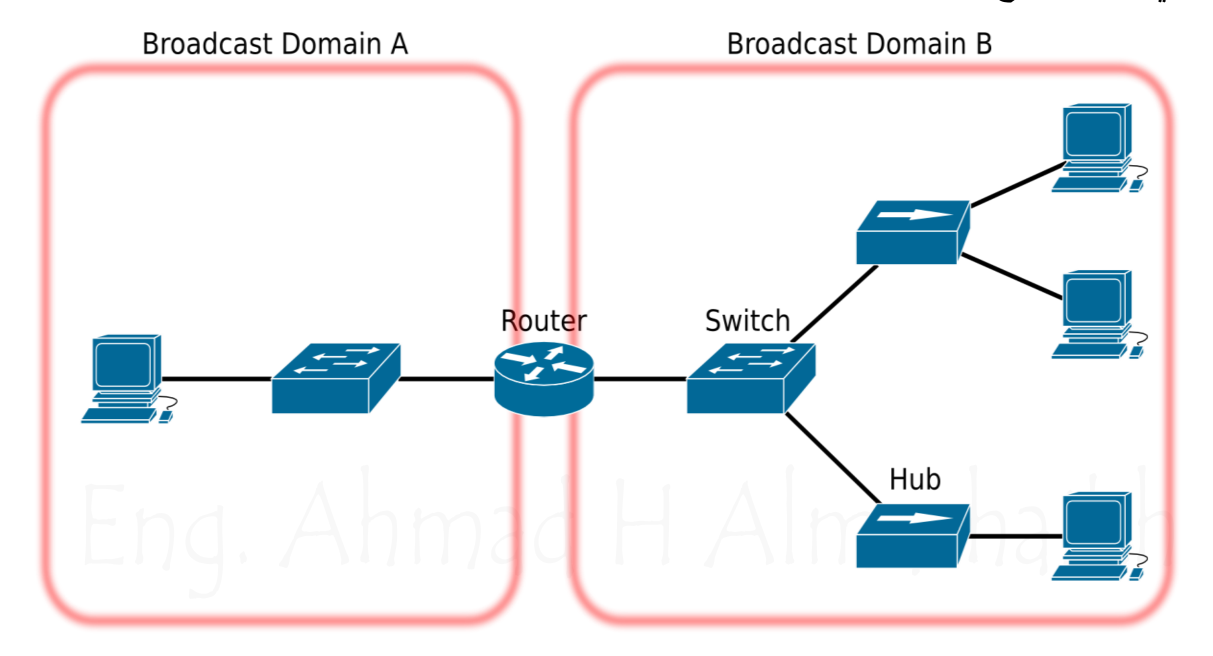




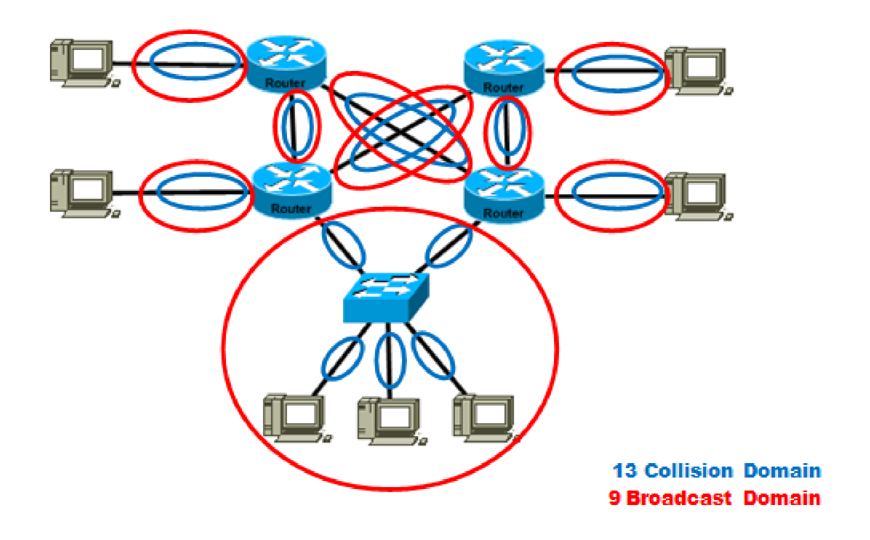
- نموذج يعرض أكثر من جهاز : جهاز سويتش و جهاز هاب و جهاز راوتر الأن الراوتر يقوم بكسر مجال البث المباشر و كل انترفيس موجودة في الراوتر تعد مجال تصادم و مجال بث مباشر مثل الصورة التالية يظهر فيها راوتر واحد تم ربط ٢ انترفيس الأن يوجد لدنيا مجال بث مباشر **A و B** .

- في هذا النموذج يوجد Broadcast A and B و يوجد 3 Collision Domain .
  - Broadcast Domain **2**
  - Collision Domain **5**

  في هذا النموذج عليك انت أن تعرف و تحلل كما عدد الـ **CD** و كما عدد **BD** :



النموذج التالي أكثر تعيقد ولكن موضح فيه من هو الـ **Collision Domain** و **Broadcast Domian**.



التصميم الهرمي لشبكات سيسكو

Cisco Three Layers Hierarchical Model

شركة سيسكو تقوم بتصنيع الأجهزة الخاصة في الشبكات على شكل مستويات و تاتي هذه المستويات على شكل هرم من اسفل إلى الاعلى ولكل مستوى وظيفته الاساسية و يتم اختيار هذه الأجهزة على شكل تصميم الشبكة و ماذا تحتاج .

تم تقسيم هذه المستويات على ثلاث مراحل :

طبقة الوصول	**1- Access Layer**
طبقة التوزيع	**2- Distribution Layer**
طبقة قلب الشبكة	**3- Core Layer**

سأقوم بشرح كل من هذه المستويات بشكل مفصل :

١- **طبقة الوصول Access Layer :** هذه الطبقة من اسمها تستخدم للوصول إلى مصدر الشبكة , و يوجد فيها غالباً الأجهزة التي يتعامل معها المستخدمين مثل أجهزة الحاسوب و الطابعات و الهاتف الخاصة في الشبكة و يتم ربط هذه الأجهزة في هذه الطبقة بشكل مباشر .

- لا يمنع هذا وجود الأجهزة و المعدات الشبكية التي تصل ما بين تلك الطرفيات مثل السويتشات و الراوترات و الاكسس بوينت الخاص بالشبكات الاسلكية .

٢- **طبقة التوزيع Distribution Layer :** هذه الطبقة تندمج فيها الطبقة السفلي طبقة الوصول **Access Layer** و هي تتعامل بشكل اساسي مع شبكة الـ (**Vlan**) و التي سنقوم بشرحها في الدروس القادمة و هي التي فيه يتم التحكم في مرور البيانات .

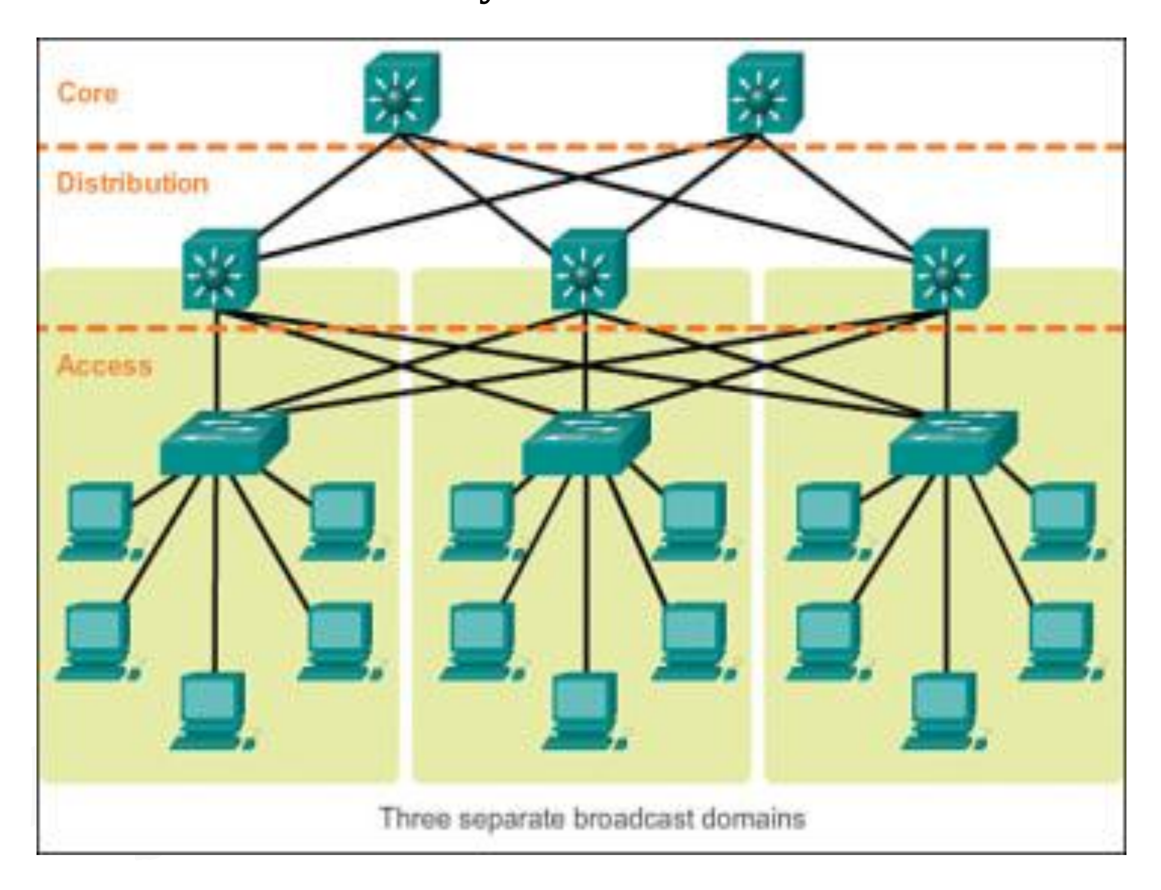
٣- **طبقة قلب الشبكة Core Layer :** هذه الطبقة تختص في تجميع البيانات من الطبقة السفلي **Distribution** بواسطة أجهزة شبكة عالية السرعة حيث إنها تتعامل مع كم هائل من البيانات المتدفقة .

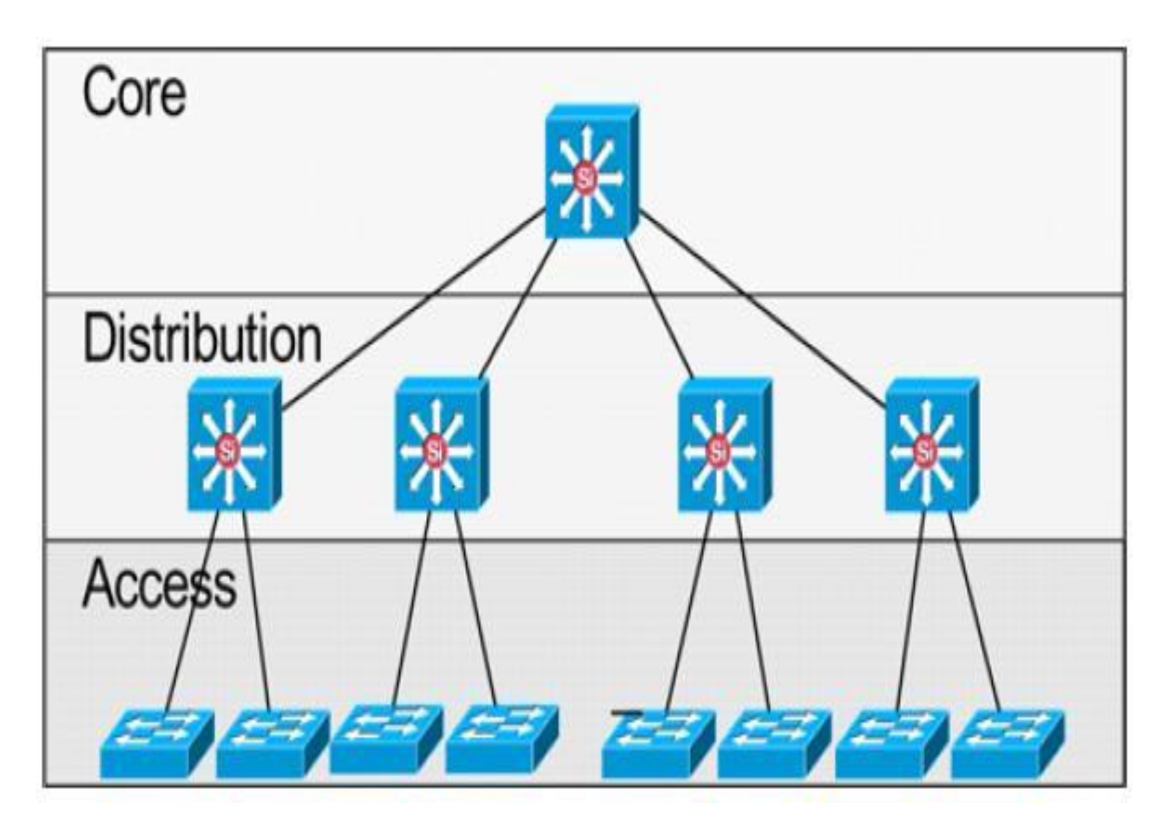
موديل أجهزة سيسكو التي تعمل في كل الطبقة :

CORE Layer	DISTRIBUTION Layer	ACCESS Layer
6500 switches	**4000 switches**	**700 routers**
8500 switches	**3600 routers**	**1900 Switches**
12000 router	**4000 routers**	**2820 Switches**
6500 switches	**4000 switches**	**1700 routers**

التصميم الهرمي لشبكات سيسكو

Cisco Three Layers Hierarchical Model





العنوان المنطقي الإصدار الرابع و السادس

IP Address - IPv4 / IPv6

Internet protocol

IPv4 / IPv6

العنوان المنطقي الـ **IPv4 Address** هو عنوان يتم توزيعها على الحواسيب ليتم تعريف الحواسيب على الشبكة و يكون لكل حاسوب عنوان على الشبكة ليستطيع مشاركة باقي الحواسيب الآخر التي على الشبكة .

- العنوان المنطقي الإصدار الرابع و هو بحجم **32 bit** يتم تقسيمها على أربع خانات كل خانة يطلق عليها **Octet** و كل خانة بحجم ثمانية بت و ينقسم إلى قسمين قسم لعنوان الشبكة و قسم لعنوان الجهاز في داخل الشبكة .
- ويجب أن نعرف أن كل خانة من الخانة الاربعة تحتوي على **8** اصفار و تبداء من صفر حتى **255** ، سأقوم بشرح هذا الموضع لنفهم كيف يتكون من اربعة خانة و كل خانات تحتوي على **8** اصفار .
- في البداية يجب أن نعرف أن عنوان الاي بي يتكون من **bit** و **Byte** و بعد عملية التكوين سيكون نظام العناوين الـ **IP** على هيئة نظامين النظام العشري أو النظام الثنائي و سأقوم بشرح هذا النظام بالتفصيل .

- **البت Bit** : هو عبارة عن رقم واحد بمعنى رقم ثنائي واحد، يكون **0** أو **1** و هذه القيمة تعتبر أصغر قيمة حاملة أو ناقلة للمعلومات، في الطبقة الفيزيائية من طبقة الـ **OSI**.

- **البايت Byte** : هو عبارة عن تجميع اكثر من رقم واحد من البت ليصبح بايت ، مثل لو تم جمع **8** اصفار في خانة واحدة هذه الخانة تعتبر بايت سأقوم بتوضيح اكثر الان، البت كما قلنا سابقاً هي عبارة عن رقم واحد اما **0** أو **1** الأن لو قمنا بجمع **8** اصفار سيتكون لدينا خانة بايت كما في المثال التالي :

- **(00000000)** الأن هذه الخانة يوجد فيها **8** اصفار هذا يعني أن هذه الاصفار ستكون **8** بايت الأن بهذا المثال يجب أن نكون فهمنا ما الفرق بين الـ **Bit** و **Byte** و فهمنا كيف يتكون عنوان الاي بي، الأن يجب أن نتذكر كما قلنا سابقنا أن عنوان الاي بي الإصدار الرابع مكون من اربعة خانات و بحجم **32** بايت بهذا الشكل يجب أن نكون فهمنا.

- الأن كما تعرفنا ساقباً إنه عنوان الـ **IP** بعد أن يتكون من البت و البايت سيتم الانتقال الى النظام العشري أو الثنائي ، و سنتعرف عليهم بشكل مبسط .

١- النظام الثنائي **Binary System:** و هو النظام الذي يتعامل مع الخانة بشكل **0** أو **1** حيث يقوم بتقسيم الخانات الى اربعة خانات كما في المثال التالي :

Octet 8 bits Octet 8 bits Octet 8 bits Octet 8 bits

00000000.00000000.00000000.00000000

11111111.11111111.11111111.11111111

هذه شكل عنوان الـ **IP** بنظام الثنائي و كل خانة بحجم **8** بايت و إذا قمنا بجمع الاربعة خانة هذه سيكون الناتج **32** بايت ، الأن بهذا الشكل نكون قد فهمنا النظام الثنائي .

٢- النظام العشري **Decimal System :** وهو النظام الذي يتعمل مع الخانة بشكل ارقام تبداء من **0** حتى **255**، و هذا النظام ايضاً يقوم بتقسيم الخانات على اربعة خانات كما في المثال التالي :

0.0.0.0

255.255.255.255

هذا شكل عنوان الـ **IP** بنظام العشري ويتم ايضاً تقسيم الخانات الى اربعة خانات كل خانة بحجم **8** بايت و إذا قمنا بجمع هذه الخانات سينتج لدينا ايضاً **32** بايت ، ولكن في النظام العشري يقوم باختصار الاصفار بدل من كتابة **8** اصفار في الخانة الواحد سيتم كتابة صفر **0** واحد في الخانة الواحدة و هذا الصفر يعبر عن **8** اصفار في النظام الثنائي كما في المثال التالي :

0.0.0.0 هذا شكل عنوان الـ **IP** في النظام العشري و مقابل له في النظام الثنائي يكون بهذا الشكل **00000000.00000000.00000000.00000000** هذا شكل الاصفار في النظام الأول و الثاني.

255.255.255.255 هذا شكل عنوان الـ **IP** ايضاً في النظام العشري و مقابل له في النظام الثنائي يكون بهذا الشكل **11111111.11111111.11111111.11111111** هذا شكل الواحد في النظام الأول و الثاني.

- بهذه الطريق يجب أن نعرف إنه هذه الارقام تساوي بعضها البعض كما في التوضيح التالي:

255.255.255.255 = 11111111.11111111.11111111.11111111

0.0.0.0 = 00000000.00000000.00000000.00000000

فئات العناوين المنطقية IP Address Class

- يوجد خمسة فئات من العناوين A , B , C , D , E
- ولكن سيتم فقط أستخدام فئات A , B , C اما بنسبه لـ فئات D , E يتم استخدامهم في اعمال اخرى مثل :
- يتم استخدام A و B و C للوصول لشبكة الانترنت ولكل فئة نطاق معين تم شرح هذه الفئة في الجدول التالي .
- **Class D:** خاصة بمجموعات الإرسال المتعدد.
- **Class E:** مخصصه لأي استخدامات مستقبلية أو بغرض البحث والتطوير.

الأن سأقوم بشرح الفئات A , B , C , D , E كما في الجدول التالي :

IP Address Classes

Address Class	1st octet range (decimal)	1st octet bits (green bits do not change)	Network(N) and Host(H) parts of address	Default subnet mask (decimal and binary)	Number of possible networks and hosts per network
A	1-127**	00000000-01111111	N.H.H.H	255.0.0.0	128 nets (2^7) 16,777,214 hosts per net (2^24-2)
B	128-191	10000000-10111111	N.N.H.H	255.255.0.0	16,384 nets (2^14) 65,534 hosts per net (2^16-2)
C	192-223	11000000-11011111	N.N.N.H	255.255.255.0	2,097,150 nets (2^21) 254 hosts per net (2^8-2)
D	224-239	11100000-11101111	NA (multicast)		
E	240-255	11110000-11111111	NA (experimental)		

** All zeros (0) and all ones (1) are invalid hosts addresses.

- الأن هذا الجدول يوضح أنواع الفئات في عنوان الـ IPv4 ، و الأن سنقوم بتحليل كل فئة من هذه العناوين لنتعرف على مدى كل عنوان IP و نتعرف على كيفية تقسيمه ، و نتعرف ايضاً على بداية و نهاية العناوين .

Class A : يبدىء عنوان الفئة A من 1 حتى 126 مع العلم إنه يبدىء من 0 حتى 127 ولكن تم حجز الـ 0 و الا 127 لوظيفة اخرى لهذا السبب يبدىء عنوان الفئة A بتوزيع من 1 حتى 126 ، و سنتعرف لماذا تم حجز الـ 0 والا 127 فيما بعد .

- الأن ناتي لنتعرف على تقسيم عنوان الفئة **A** ينقسم الى اربع اقسام القسم الأول لعنوان الشبكة، ويبقى ثلاث اقسام لعنونة الأجهزة كما في المثال التالي :

N. H. H. H

10.0.0.0

- رمز **N** اختصار لـ **Network** و **H** اختصار لـ **Host** هذا يعني أن أول خانة من عنوان الفئة **A** مخصصة لعنون الشبكة و باقي الخانات لعنون الجهاز ، وبهذا الشكل يتكون لدينا عدد شبكات من عنوان الفئة **A 126** شبكة و عدد الأجهزة سيكون **16,777,216** جهاز .

- عنوان الـ **Subnetmask** لعنوان الفئة **A** سيكون **255.0.0.0** هذا الطبيعي و من غير تقسيم لعنون الشبكة كما سنتعرف في الدروس القادمة عن كيفية تقسيم الـ**Subnetmask**.

Class B : يبداء عنوان الفئة **B** من **128** حتى **191** .

- الأن ناتي لنتعرف على تقسيم عنوان الفئة **B** ينقسم الى اربع اقسام القسم الأول والثاني لعنوان الشبكة, ويبقى قسمين لعنونة الأجهزة كما في المثال التالي :

N. N. H. H

150.1.0.0

- رمز **N** اختصار لـ **Network** و **H** اختصار لـ **Host** هذا يعني أن أول و ثاني خانة من عنوان الفئة **B** مخصصة لعنونة الشبكة و باقي الخانات لعنون الجهاز ، وبهذا الشكل يتكون لدينا عدد شبكات من عنوان الفئة **B 65,534** شبكة و عدد الأجهزة سيكون **16,384** جهاز .

- عنوان الـ **Subnetmask** لعنوان الفئة **B** سيكون **255.255.0.0** هذا الطبيعي و من غير تقسيم لعنون الشبكة .

Class C : يبداء عنوان الفئة **C** من **192** حتى **223** .

- الأن ناتي لنتعرف على تقسيم عنوان الفئة **C** ينقسم الى اربع اقسام القسم الأول والثاني و الثالث لعنوان الشبكة, ويبقى قسم واحد لعنونة الأجهزة كما في المثال التالي :

N. N. N. H

192.168.1.0

- رمز **N** اختصار لـ **Network** و **H** اختصار لـ **Host** هذا يعني أن أول و ثاني وثالث خانة من عنوان الفئة **C** مخصصة لعنونة الشبكة و الخانة الاخيرة لعنون الجهاز ، وبهذا الشكل يتكون لدينا عدد شبكات من عنوان الفئة **C 2,097,152** شبكة و عدد الأجهزة سيكون **255** جهاز .

- عنوان الـ Subnetmask لعنوان الفئة C سيكون 255.255.255.0 هذا الطبيعي و من غير تقسيم لعنون الشبكة .

- الأن بعد أن تعرفنا على فئات العناوين ، سنقوم بتعرف على عملية التحويل ما بين النظام العشري و النظام الثنائي في العناوين.

- الأن قبل أن نبداء في التعرف على عملية التحويل اريد أن اوضح نقطة مهم جداً يجب علينا أن نفهم هذه العملية بشكل جيد جداً ، و هذه العملية مهم جداً أن نكون على معرفة كيفية التحويل ما بين النظام العشري و النظام الثنائي لنكون على فهم و معرف بشكل ممتاز عن كيفية عملية التحويل كيف تتم و كيف يتكون عنوان الـ IP من خلال النظام العشري و النظام الثنائي .

- في البداية يجب أن نتذكر اننا قمنا بتعرف مسبقاً على النظام العشري و النظام الثنائي و تعرفنا على إنه كل خانة من خانة العنوان تتكون من 8 byte و تم تجميعهم من 8 bit ، و الأن يجب أن نعلم قبل أن نبداء في عملية التحويل يجب انعرف إنه يوجد جدول مكون من 8 ارقام و هذا الجدول هو الذي يتكون منه عنوان الـ IPو هو المستخدم في عملية التحويل ما بين النظام العشري و النظام الثنائي ، الأن ناتي لنعرف كيف يتكون هذا الجدول و كيف تم تجميعها .

128 64 32 16 8 4 2 1

هذا هو الجدول الذي سنقوم من خلالها في عملية التحويل ما بين النظام العشري و النظام الثنائي ، مع العلم إنه هذا الجدول مكتوب بنظام العشري .

ملاحظة مهم جدا جداً : هذا الجدول يمثل خانة واحد من اربعة خانة في عنوان الـ IP .

الأن لنتعرف كيف تم جلب هذا الجدول ، هذا الجدول ياتي من بعد عملية حسابية نقوم بضرب الاعداد من خلال الـ اوس و ينتج لدنيا هذا الجدول سنقوم بتعرف على العملية الحسابية لي اظهار هذا الجدول المكون من 8 ارقام .

تبداء العملية الحسابية من الرقم 0 حتى الرقم 7 لينتج لدنيا هذا الجدول كم في المثال التالي:

2^0 = 1

2^1 = 2

2^2 = 4

2^3 = 8

2^4 = 16

2^5 = 32

2^6 = 64

2^7 = 128

A Single Byte

2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
128	64	32	16	8	4	2	1
1	1	1	1	1	1	1	1
128	+64	+32	+16	+8	+4	+ 2	+ 1

=255

is the largest decimal value that can be expressed in 8 bits.
How many different patterns are there?

- الأن بعد أن تعرفنا على كيفية استخراج الجدول ناتي لتوضيح الجدول كما هو موجود في الصورة :

هذا العدد العشري 128 64 32 16 8 4 2 1

هذا العدد الثنائي 1 1 1 1 1 1 1 1

- الأن لو قمنا بجمع الارقام التي في الجدول سيتنج لدنيا العدد **255** و هذا يدل على إنه كل خانة بحجم **8 byte** كما في التوضيح التالي :

255 = 128 + 64 + 32 + 16 + 8 + 4 + 2 + 1

بهذا الشكل يكون قد تم توضيح الجدول و كيف يتم جمعها و كيف الخانة تتكون ، الأن لو قمنا بجمع نفس هذه القيمة على اربعة خانات سيخرج لدينا على الاربع خانات هذه القيمة :

255.255.255.255

هذه القيمة التي تم حسابه على الاربع خانة ولو قمنا بحسب الاربع خانات على شكل الـ **8 byte** سيكون حجم العنوان **32 byte** .

- الأن ناتي لعملية التحويل ما بين النظام العشري و النظام الثنائي سأقوم بشرح عملية التحويل بشكل مبسط لنستطيع فهم عملية التحويل و سناخذ اكثر من مثال .

- مثال على العنوان التالي **192.168.50.1** هذا العنوان مكتوب بنظام العشري ، و نريد تحويله من النظام العشري الى النظام الثنائي سنقوم بفرد الجدول المكون من **8** ارقام و نبداء بعملية التحويل تابع الخطوات التالية .

١- سنقوم بفرد جدول الارقام بنظام العشري و النظام الثنائي .
٢- سنقوم بعملية الجمع من جدول الارقام التي بنظام العشري و نحوله للنظام الثنائي و هو الذي سيكون **0** أو **1** .
٣- سنبداء في عملية تحويل كل خانة بمفرده لنفهم كيف ستتم عليمة الاستخراج .

- الأن سنبداء في عملية الاستخراج و التحويل :

هذا العدد العشري 128 64 32 16 8 4 2 1

هذا العدد الثنائي 1 1 0 0 0 0 0 0

- الأن نريد اخراج و تحويل قيمة الخانة **192** سنقوم بنظر على جدول العدد العشري نريد أن نستخرج منه عدد **192** سنقوم بعملية الجمع كتالي ، رقم **192** اكبر من **128** هذا صحيح ولكن سنقوم باخذ الـ **128** و نقوم بوضع رقم **1** اسفل الـ **128** كما في الجدول اعلى ، الأن قمنا بجمع **128** من **192** نريد أن نستكمل العملية لنستخرج **192** ما هو الرقم الذي سيكمل رقم الـ **192** من الطبيعي جداً إنه رقم **64** سنقوم بوضع رقم **1** ايضاً اسفل الـ **64** , ولو قمنا بعملية الجمع ما بين **192 =128 + 64** بهذه الطريقة

نكون قد استخرجنا أول خانة من خانة العنوان و هي الـ **192** ولا ننسا أن نقوم باكمل وضع الاسفار اسفل الارقام المتبقية في الجدول أنظر للجدول اعلى إذا لم تستوعب الفكره ، بعد أن قمت بنظر سترى إنه فقط تم جمع رقمين لعملية اخرج رقم الـ **192** و هما **128 + 64** سنقوم بوضع رقم **1** تحتهم و باقي الارقام ستكون اصفر، بهذه الطريق قمنا بعملية جمع و استخراج و عملية تحويل ايضاً ما بين النظام العشري و النظام الثنائي .

هذا العدد العشري 128 64 32 16 8 4 2 1

هذا العدد الثنائي 1 0 1 0 0 0 0 0

- الأن ناتي للخانة الثانية و هي **168** سنقوم بنفس الطريقة الأولى سننظر للجدول ، و نرى ما هي الارقام التي إذا قمنا بجمعهم سيخرج لنا **168** ، من الطبيعي جداً إذا نظرنا الى رقم الـ **128** و نظرنا ايضاً لرقم الـ **64** و قمنا بعملية الجمع سينتج رقم اكبر من **168** ، في هذه الحالة سنقوم بموعدة النظر مره اخرى سنقوم باخذ رقم الـ **128** و **32** و **8** ولو قمنا بجمع هذه الارقام **168 = 8 + 32 + 128** بهذه الطريقة نكون قد اخرجنا قيمة الخانة الثانية **168** ، و يجب أن لا ننسى أن نقوم بوضع رقم **1** اسفل الارقام التي اخذنها و هي **128** و **32** و **8** كما في الجدول اعلى .

هذا العدد العشري 128 64 32 16 8 4 2 1

هذا العدد الثنائي 0 0 1 1 0 0 1 0

- الأن ناتي للخانة الثالثة و هي **50** سنقوم بنفس الطريقة الأولى سننظر للجدول ، و نرى ما هي الارقام التي إذا قمنا بجمعهم سيخرج لنا **50** ، من الطبيعي جداً سنقوم بنظر على رقم **32** و **16** و **2** سنقوم بعملي جمع لنرى هل سيخرج لنا الناتج **50** أو اكثر أو اقل **50=2 + 16 + 32** نرى بعد عملية الجميع إنه الناتج **50** في هذه الحالة سنقوم بوضع رقم **1** تحت الارقام التالية التي قمنا بجمعها و هي **32 , 16 , 2** و باقي الارقام سنقوم بوضع رقم **0** اسفلها و هي التي لم تدخل في عملية الجميع .

هذا العدد العشري 128 64 32 16 8 4 2 1

هذا العدد الثنائي 0 0 0 0 0 0 0 1

- الأن ناتي للخانة الرابع و هي **1** رقم واحد و هو موجود في الجدول ولا يحتاج الى عملية ضرب أو حساب بكل بساطة سنقوم باخذ رقم **1** ، و نقوم بوضع رقم واحد اسفل الرقم المختار و باقي الارقام ستكون **0** ، كما في الجدول اعلى .
- الأن بعد أن تعرفنا على عملية الجمع و عملية استخراج العنوان يجب أن نكون على معرفة عن كيفية التحويل بشكل ممتاز ، و سأقوم الأن بذكر بعض الامثلة لنكون قد تم فهم عملية التحويل بشكل ممتاز :

سنقوم بتحويل العنوان طبعاً بعد أن تم تجميعه من الجدول المكون من **8** ارقام سنقوم بتحويله من النظام العشري الى النظام الثنائي و العكس تابع المثال مع الشرح المبسط :

- هذا العنوان الذي قمنا بمعرفة تكوينه **192.168.50.1** الأن بهذا الشكل مكتوب بنظام العشري ، و نريد أن نقوم بمعرفة شكله بنظام الثنائي ، سيكون كتالي :

النظام العشري Decimal System :192.168.50.1

النظام الثنائي Binary System: 11000000. 10100000.00110010.00000001

- **عنوان من الفئة B 172.16.1.1 نريد ايضاً فهمه :**

النظام العشري Decimal System :172.16.1.1

النظام الثنائي Binary System: 10101100. 00010000.00000001.00000001

- **عنوان من الفئة A 126.50.1.1 نريد ايضاً توضيحه :**

النظام العشري Decimal System :126.255.240.20

النظام الثنائي Binary System: 01111110.11111111.11110000.00010100

- الأن بعد أن قمنا بعملية التحويل و الجمع و الاستخراج بهذا الشكل نكون قد فهمنا كيف يتكون عناون الـ **IP** و اريد أن انصحكم في نقطة مهم جداً جداً جداً الجدول التالي اتمنى انكم تفهموه و تحفظوه بشكل ممتاز لي إنه سيسهل عليك عملية التحويل و الجميع و استخراج العنوان لكل خانة :

00000000 = 0
10000000 = 128
11000000 = 192
11100000 = 224
11110000 = 240
11111000 = 248
11111100 = 252
11111110 = 254
11111111 = 255

أنواع العناوين المنطقية الخاصة IPv4

١- العناوين المنطقية الخاصة Private IPv4 Address

يوجد أكثر من نوع من العناوين المنطقية و يتم تقسيم هذه العناوين على حسب تصميم الشبكات و ماذا تحتاج الشبكة من أنواع العناوين المنطقية .

١- الفئة A : 1.0.0.0 حتى 126.255.255.254
٢- الفئة B : من 172.16.0.0 حتى 172.31.255.254
٣- الفئة C : 192.168.0.0 حتى 192.168.255.254
٤- الفئة D : 239.0.0.0

٢- عنوان كرت الشبكة الداخلي Loop Back Interface ولا يمكن استخدامه في عنونة الشبكات ، فقط هذا محجوز لكرت الشبكة .

127.0.0.1

٣- العنوان الخاص التلقائية الذي يسيمى APIPA هو عنوان مؤقت ياتي بعد عدة مراحلة من استلام عنوان IP .

APIPA = Automatic Private IP Addressing

169.254.0.0

٤- العناوين المحجوزة في الفئة E : تبداء من 239 حتى 254

٨- عنوان البث المتعدد المحجوز للبث المتعدد الخاص بالشبكة ، و يستخدم ايضاً مع بعض البروتوكولات .

Reserved Multicast Address 224.0.0.0

٦-عنوان البث العام General Broadcast Address

255.255.255.255

يستخدم هذا العنوان عندما نريد إرسال بيانات لكل الشبكة .

٧- العناوين العامة و هي العناوين التي يستخدمها شركات مزودي الخدمة ISP لتوزيع العناوين على المشتركين و ليستطيعوا الاشتراك في خطوط الانترنت و هذه العناوين تمسى العناوين العامة Public IP Address و هذا العناوين يكون عام على شبكة الانترنت .

ملاحظة : لا يمكن أستخدام العناوين الخاصة التي نقوم بتركيبه على الشبكة المحلية في داخل المنزل أو الشركة أو المؤسسة أن نستخدمه مثل العناوين العامة التي تكون على الانترنت هذه العناوين فقط تستخدم في الشبكة الخاصة و المحلية بمعنى الشبكة الداخلية فقط و لا يمكن استخدامها لدخول على شبكة الانترنت .

Class Full / Class Less

قيمة الوحايد للشبكة	قناع الشبكة	المدى	الفئة
/8	255.0.0.0	0-127	Class A
/16	255.255.0.0	128-191	Class B
/24	255.255.255.0	192-223	Class C
/8	255.0.0.0	224-239	Class D

- **الأن سأقوم بشرح كل من Class Less / Class Full و معرفة الفرق ما بينهم :**
- **Class Full :** هي قيمة الوحايد للشبكة التي لم يتم التغير فيها مثل يوجد لدينا عنوان **ip: 10.0.0.0 / 8** قيمة الوحايد للشبكة هي **/8** كما هو موجود في الجدول و هذا يعني إنه لا يوجد استخدام لتقسيم الشبكة و لم يتم التغير أو التلعب في عنوان الـ **ip** في هذه الحالة تسمى **Class Full** .
- **Class Less :** هي قيمة الوحايد للشبكة التي تم التغير و التقسيم فيها و تم العمل عليه من قبل الـ **Subnetting** أو الـ **VLSM** و سنقوم بشرح هذه العملية في الدروس القادمة مع العلم إنه هذه العملية هي المسؤولة عن تقسيم عناوين الشبكة و في حال تم تغير قيمة وحايد الشبكة مثل لو كان لدنيا عنوان شبكة بهذا الشكل **ip : 10.0.0.0/16** يجب أن نعرف إنه تم تقسيم هذا العنوان في هذه الحال يطلق عليه **Class Less** لإنه تم التغير في قيمة الوحايد للشبكة و سأقوم بشرح هذه العملية بشكل مميز في الدروس القادمة .
- **مميزات كل من Class Less / Class Full :**

Class Full

١- يعتمد على قاعدة الـ **IP Classes** في توزيع العناوين .
٢- لا يرسل الـ **Subnet Mask** مع التحديثات الخاصة به على الشبكة لان الماسك ثابت و معروف عند جميع الراوتر أو الموجهات .
٣- يتم عمل الغاء للـ **Packet** في حال لم يتم تطابقها مع أحد معطيات جدول الموجه **Routing Table** .

Class Less

١- يتجاهل هذه القاعدة و يتم توزيع العناوين بشكل مفتوح و يعتمد على تقنية الـ **VLSM** .
٢- يرسل الـ **Subnet Mask** مع جميع العناوين المرسلة إلى الموجهات أو الراوترات لأنه متغير المرسل و بحسب الطلب .
٣- يتم إرسال الـ **Packet** إلى الـ **Default Router** لو في حال لم يتم تطابقها مع أحد الشبكات الموجودة في جدول التوجيه .

تقسيم الشبكات
IP Subnetting

Subnetting: هي عملية تقسيم عنوان الشبكة الرئيسي إلى عدة عناوين شبكات فرعية، و الغرض من ذالك هو تقليل عملية استهلاك الـ **IP** ضمن نطاق الشبكة الرئيسية.

- مثال على استهلاك عناوين الـ **IP** عندما نقوم بتصميم شبكة و نقوم بتركيب عنوان من الفئة **A** فهذا يعني اننا قمنا باختيار عدد كبير من الأجهزة و عدد قليل من الشبكات و نحن لا نحتاج لكل هذه الشبكات ولا لكل الأجهزة ما الحل ؟ الحل هو أن نقوم باستخدام عملية تقسيم العناوين و هي عملية الـ **Subnetting** لتقوم بتقسيم عناوين الشبكات و استخدام العدد المطلوب فقط في تصميم الشبكة الذي يجب استخدامه بدل من ضياع باقي العناوان .
- فوائد تقسيم الشبكة الى اجزاء :

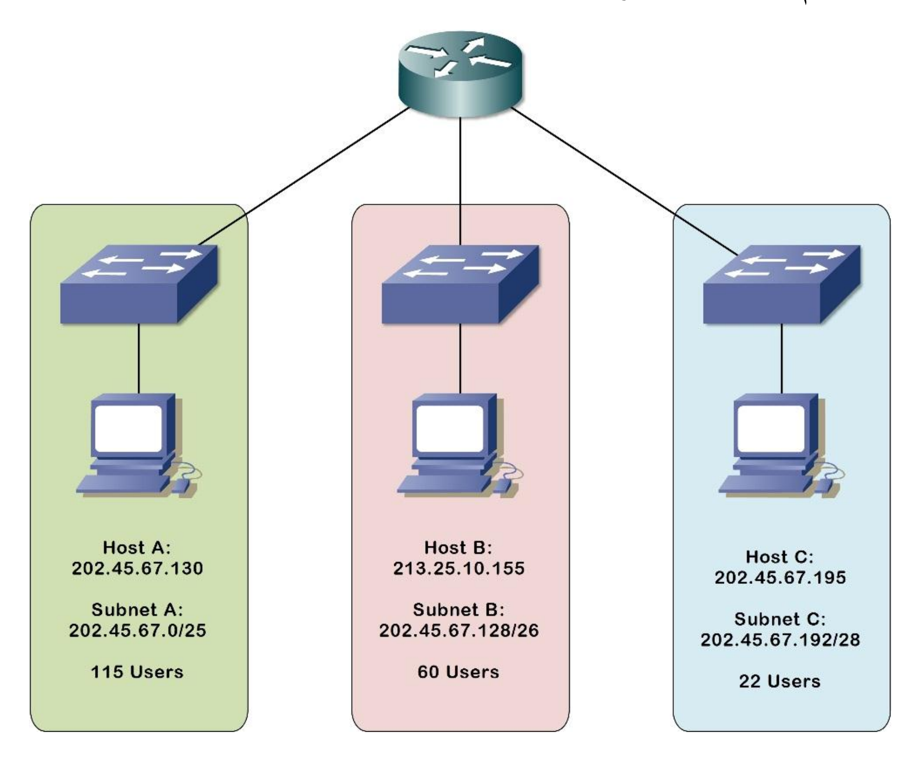
١- تقليل عملية البث المباشر الـ **Broadcast** في حال تم اختيار عنوان من الفئة التي قمنا بذكره سابقاً في انت الأن قمت باختيار العناوين و قمت بتركيب هذه العناوين على أجهزة الشبكة في هذه الحال أن قمت باستهلاك كل العناوين أو لم تقوم باستهلاك كل العناوين في نظر جهاز الموجه أو الراوتر اننا مستهلك كل العناوين في هذه الحال يحدث ثقل في الشبكة و بما يسمى البث المباشر **Broadcast** لهذا نحن نقوم بتقسيم العناوين لتقليل عملية البث المباشر و ثقل الشبكة .

٢- أفضل في مجال الحماية و الأمن في داخل الشبكة .

٣- سهولة في عملية الصيانة .

٤- سهولة في ادارة الشبكة .

٥- تصميم و تقسيم الشبكة كما نريد .



- الأن ناتي لعملية تقسيم العناون ، ولكن قبل أن نبداء يجب أن نكون على معرفة ما هو عدد الشبكات و ما هو عدد الأجهزة التي نريده قبل أن نبداء في عملية التقسيم .

- **سنبداء بتقسيم عنوان من الفئة (A) 10.0.0.0/8**

- نريد تقسيم هذا العنوان الواحد **10.0.0.0/8 255.0.0.0** الى خمسة عناوين شبكةسنقوم بفرد الجدول المكون من **8** ارقام الذي قمنا بعملية الجمع و التحويل منه في الدروس السابقة ، و الأن نريد أن نقوم بعملية التقسيم من خلال هذا الجدول .
- الأن سنقوم بعملية التقسيم سنقوم بفرد العنوان الذي نريد أن نقسمه الى خمسة عناوين شبكة ، و سنقوم ايضاً بفرد الجدول الذي يحتوي على **8** ارقام كما في المثال التالي :

10.0.0.0/8 255.0.0.0

128 64 32 16 8 4 2 1

1 1 1

- سنبداء بعملية اختيار بعض الارقام و نقوم بوضع رقم **1** تحت كل رقم مختار و بعده سنقوم بعملية الحساب عن طريق الاوس ^ بجمع ارقام الوحايد التي تحت كل رقم قمنا باختياره في الجدول لينتج لدنيا **5** شبكات .
- الأن قمنا باختيار الارقام التالية **128 , 64 , 32** و سنقوم بوضع رقم **1** تحت كل رقم من التي قمنا باختياره و سنقوم بعملية حسب الوحايد عن طريق الـ ^ كما في المثال التالي:

128 64 32 16 8 4 2 1

1 1 1

- لو قمنا بعملية الحساب كتالي **2 = 2^1** سينتج لدينا رقم **2** العدد اقل من خمسة ، ولو قمنا بعملية حساب كتالي **4 = 2^2** سينتج لدينا رقم **4** العدد ايضاً اقل من خمسة ، سنقوم بعملية حساب كتالي **8 = 2^3** سينتج لدينا رقم **8** بعملية الحساب هذه اقل شيء سينتج لدينا بمعنى إنه سيكون لدينا **8** شبكات ، نستطيع أن نقوم بحذف **3** شبكات و يتبقى لدينا 5 شبكات بهذه الطريقة قمنا بتقسيم العناون بهذا الشكل سينتج لدينا الارقام التي اليسار المميزة بالون الاحمر هي لصالح الشبكة و الارقام التي بالون الاسود لصالح عنوانة الأجهزة .
- الأن سيكون شكل قناع الشبكة **Subnet mask** بشكل هذا **255.224.0.0** بعد عملية جميع الاقام التالية **224 = 32 + 64 + 128** .
- و قيمة عدد الوحايد أو الـ **CIDR** في الطبيعي ما قبل التقسيم يكون **/8** و بعد عملية التقسيم سيكون **/11** كيف اصبح **11** بكل بساطة هو طبيعي **/8** ولو قمنا بزيادة الارقام الثلاثة التي هي رقم **11 = 8 + 1 + 1 + 1** .

:Block size هو عبارة عن حدود حجم عنوان الشبكة و آخر رقم يكون في كل شبكة و ستبداء أول شبكة باخذ الـ **Block size** برقم **32** و عند الانتقال للشبكة الثاني و هي الشبكة الجديدةسيكون الـ **64 Block size**، و سيبقى يظرب نفسه حتى يصل الى آخر شبكة من التقسيم.

الشبكة بعد التقسيم

10.0.0.0/11 255.224.0.0

عنوان الشبكة الأولى

عنوان الشبكة 10.0.0.0/11 255.224.0.0

عنوان الجهاز الأول 10. 31.0.1

عنوان الجهاز الاخير في الشبكة 10.31.255.254

عنوان البث الخاص في الشبكة الأولى 10.31.255.255

عنوان الشبكة الثانية

عنوان الشبكة 10.32.0.0/11 255.224.0.0

عنوان الجهاز الأول 10.32.0.1

عنوان الجهاز الاخير في الشبكة 10.63.255.254

عنوان البث الخاص في الشبكة الأولى 10.63.255.255

عنوان الشبكة الثالثة

عنوان الشبكة 10.64.0.0/11 255.224.0.0

عنوان الجهاز الأول 10.64.0.1

عنوان الجهاز الاخير في الشبكة 10.95.255.254

عنوان البث الخاص في الشبكة الأولى 10.95.255.255

عنوان الشبكة الرابعة

عنوان الشبكة 10.96.0.0/11 255.224.0.0

عنوان الجهاز الأول 10.96.0.1

عنوان الجهاز الاخير في الشبكة 10.127.255.254

عنوان البث الخاص في الشبكة الأولى 10.127.255.255

عنوان الشبكة الخامسة

عنوان الشبكة 10.128.0.0/11 255.224.0.0

عنوان الجهاز الأول 10.128.0.1

عنوان الجهاز الاخير في الشبكة 10.159.255.254

عنوان البث الخاص في الشبكة الأولى 10.159.255.255

عنوان الشبكة السادسة

عنوان الشبكة 10.160.0.0/11 255.224.0.0

عنوان الجهاز الأول 10.160.0.1

عنوان الجهاز الاخير في الشبكة 10.191.255.254

عنوان البث الخاص في الشبكة الأولى 10.191.255.255

عنوان الشبكة السابعة

عنوان الشبكة 10.192.0.0/11 255.224.0.0

عنوان الجهاز الأول 10.192.0.1

عنوان الجهاز الاخير في الشبكة 10.223.255.254

عنوان البث الخاص في الشبكة الأولى 10.223.255.255

عنوان الشبكة الثامنة

عنوان الشبكة 10.224.0.0/11 255.224.0.0

عنوان الجهاز الأول 10.224.0.1

عنوان الجهاز الاخير في الشبكة 10.255.255.254

عنوان البث الخاص في الشبكة الأولى 10.255.255.255

- **سنبداء بتقسيم عنوان من الفئة (C) 192.168.1.0/24**

- نريد تقسيم هذا العنوان الواحد **192.168.1.0/24 255. 255. 255.0** الى ثمانية عناوين شبكة سنقوم بفرد الجدول المكون من **8** ارقام الذي قمنا بعملية الجمع و التحويل منه في الدروس السابقة ، و الأن نريد أن نقوم بعملية التقسيم من خلال هذا الجدول .

- الأن سنقوم بعملية التقسيم سنقوم بفرد العنوان الذي نريد أن نقسمه الى خمسة عناوين شبكة ، و سنقوم ايضاً بفرد الجدول الذي يحتوي على **8** ارقام كما في المثال التالي :

192.168.1.0/24 255.255.255.0

128 64 32 16 8 4 2 1

1 1 1

- سنبداء بعملية اختيار بعض الارقام و نقوم بوضع رقم **1** تحت كل رقم مختار و بعده سنقوم بعملية الحساب عن طريق الاوس ^ بجمع ارقام الوحايد التي تحت كل رقم قمنا باختياره في الجدول لينتج لدنيا **8** شبكات .

- الأن قمنا باختيار الاقام التالية **32 , 64 , 128** و سنقوم بوضع رقم **1** تحت كل رقم من التي قمنا باختياره و سنقوم بعملية حسب الوحايد عن طريق الـ ^ كما في المثال التالي:

128 64 32 16 8 4 2 1

1 1 1

- لو قمنا بعملية الحساب كتالي **2^1 = 2** سينتج لدينا رقم **2** العدد اقل من ثمانية ، ولو قمنا بعملية حساب كتالي **2^2 = 4** سينتج لدينا رقم **4** العدد ايضاً اقل من ثمانية ، سنقوم بعملية حساب كتالي **2^3 = 8** سينتج لدينا رقم **8** بعملية الحساب هذا هو المطلوب على عدد الشبكة بتمام ، بمعنى إنه سيكون لدينا **8** شبكات بهذه الطريقة قمنا بتقسيم العناون بهذا الشكل سينتج لدينا الارقام التي اليسار المميزة بالون الاحمر هي لصالح الشبكة و الارقام التي بالون الاسود لصالح عنوانة الأجهزة .

- الأن سيكون شكل قناع الشبكة **Subnet mask** بشكل هذا **255.255.255.224** بعد عملية جميع الاقام التالية **224 = 32 + 64 + 128** .

- و قيمة عدد الوحايد أو الـ **CIDR** في الطبيعي ما قبل التقسيم يكون **24/** و بعد عملية التقسيم سيكون **27/** كيف اصبح **27** بكل بساطة هو طبيعي **24/** ولو قمنا بزيادة الارقام الثلاثة التي هي رقم **27 = 24 + 1 + 1 + 1** .

- العملية نفس العملية الأولى التي قمنا بتقسيم العنوان من الفئة **A** ولكن يختلف بعض الشيء في العناوين فقط ولكن نفس العملية و نفس الطريق لان يختلف شيء عنها .

الشبكة بعد التقسيم

192.168.1.0/27 255. 255. 255.224

عنوان الشبكة الأولى

عنوان الشبكة 192.168.1.0/27 255.255.255.224

عنوان الجهاز الأول 192.168.1.1

عنوان الجهاز الاخير في الشبكة 192.168.1.30

عنوان البث الخاص في الشبكة الأولى 192.168.1.31

عنوان الشبكة الثانية

عنوان الشبكة 192.168.1.32/27 255.255.255.224

عنوان الجهاز الأول 192.168.1.33

عنوان الجهاز الاخير في الشبكة 192.168.1.62

عنوان البث الخاص في الشبكة الأولى 192.168.1.63

عنوان الشبكة الثالثة

عنوان الشبكة 192.168.1.64/27 255.255.255.224

عنوان الجهاز الأول 192.168.1.65

عنوان الجهاز الاخير في الشبكة 192.168.1.94

عنوان البث الخاص في الشبكة الأولى 192.168.1.95

عنوان الشبكة الرابعة

عنوان الشبكة 192.168.1.96/27 255.255.255.224

عنوان الجهاز الأول 192.168.1.97

عنوان الجهاز الاخير في الشبكة 192.168.1.126

عنوان البث الخاص في الشبكة الأولى 192.168.1.127

عنوان الشبكة الخامسة

عنوان الشبكة 255.255.255.224 192.168.1.128/27

عنوان الجهاز الأول 192.168.1.129

عنوان الجهاز الاخير في الشبكة 192.168.1.158

عنوان البث الخاص في الشبكة الأولى 192.168.1.159

عنوان الشبكة السادسة

عنوان الشبكة 255.255.255.224 192.168.1.160/27

عنوان الجهاز الأول 192.168.1.161

عنوان الجهاز الاخير في الشبكة 192.168.1.190

عنوان البث الخاص في الشبكة الأولى 192.168.1.191

عنوان الشبكة السابعة

عنوان الشبكة 255.255.255.224 192.168.1.192/27

عنوان الجهاز الأول 192.168.1.193

عنوان الجهاز الاخير في الشبكة 192.168.1.222

عنوان البث الخاص في الشبكة الأولى 192.168.1. 223

عنوان الشبكة الثامنة

عنوان الشبكة 255.255.255.224 192.168.1.224/27

عنوان الجهاز الأول 192.168.1.255

عنوان الجهاز الاخير في الشبكة 192.168.1.254

عنوان البث الخاص في الشبكة الأولى 192.168.1.255

IPv6

Internet Protocol Version 6

- العنوان المنطقي الإصدار السادس و هو بحجم **128 bit** يتم تقسيمها على ثمانية خانات كل خانة يطلق عليها **Octet** و كل خانة بحجم **16** بت و ينقسم إلى قسمين قسم لعنوان الشبكة و قسم لعنوان الجهاز في داخل الشبكة ، ويعتمد على نظام الـ **hexadecimal** و هو النظام السادس عشر و يتكون من **16** رقم يعمل فيه عنوان الإصدار السادس **IPv6**.

IPv6 : هو تطوير لعنوان الإنترنت الإصدار الرّابع (**IPv4**) هذا الإصدار الجديد **IPv6** يأتي في نفس الوقت بالعديد من التّمديدات والتّحسينات والتّكميلات لقدرات الإصدار الرّبع (**IPv4**) .

مميزات عنوان الإصدار السادس الـ IPv6 :

١- لا يوجد في عنوان الإصدار السادس البث المتعدد الـ **BroadCast** الموجود في الإصدار الرابع ، و تم تطوير خاصية الـ **Any Cast** التي قمت بشرحها في الدروس السابقة ، و هذه الخاصية قد حلت مشاكل كثير كانت موجودة في الإصدار الرابع .

٢- عنوان الإصدار السادس أكثر أمان من الإصدار الرابع ، و تم إضافة خاصية الـ **IPsec** بشكل تلقائي و مفعل من دون أن نقوم بتفعيله نحن مثل الإصدار الرابع الذي كنا نقوم بتفعيل خاصية الـ **IPsec** عليه .

٣- تقديم حماية أفضل للمعلومات مثل المصداقية و الخصوصية التي غير موجود في الإصدار الرابع .

٤- يحتوي على المميزات الموجودة في الإصدار الرابع حيث إنه تم دمج المميزات القديمة التي في العنوان القديم تم دمجه في العنوان الجديد الإصدار السادس ليعمل بشكل مميز.

٥- مراحل تكوين العناوين الـ **IP Header v6** تختلف عن الـ **IP Header v4** و سنقوم بشرح الـ **IP Header** بالتفصيل في الدروس القادمة .

٦- يعمل مع البروتوكولات التالية بشكل طبيعي جداً مثل : **DNS** , **BGP**, **OSPF**, **TCP**, **UDP** , **IGMP**, **EIGRP** ,**RIPng**، **DHCP**.

٧- يوفر عدد كبير جدا من العناوين ما يقارب **340** تريليون تريليون تريليون عنوان بينما ، الإصدار الرابع كان يوفر عدد اقل منه حوالي **4.3** مليار عنوان .

أنواع إرسال البيانات في العناوين السادس IPv6 :

Unicast, Multicast, Any Cast

و هي التي قمت بشرحها بالتفصيل في الدورس السابقة ، ولكن يجب أن نعلم أن الـ **BroadCast** تم حذفها من الإصدار السادس و تم إضافة الـ **Any Cast** بدالها .

شكل عنوان الـ IPv6 fec80:0000:0000:0000:0c41:1536:3f57:fef5

نلاحظ إنه مقسم الى قسمين قسم بالون الاحمر و قسم بالون الازرق القسم الأول الذي بالون الاحمر حجمه **64 bit** و هو خاص بعنوان الشبكة **Network ID** ، و القسم الثاني الذي بالون الازرق حجمه ايضاً **64 bit** و هو خاص بعنوان الأجهزة **Host**.

- كيف نستطيع أن نقراء العنوان بشكل سهل ، يوجد عدة طرق لجعل قراءة العناوين سهل وتسمى هذه الطرق بصيغة العنوان المنطقي الإصدار السادس **IPv6 Address Format** سأقوم بشرحه لنفهم كيفية تحليله :

2005:0005:0100:0000:0000:0000:0000:070

- هذا شكل العنوان السادس ما قبل أن نقوم بتغير فيه أنظر اليه كامل ، و الأن نريد أن نقوم بحذف خانات الاصفر المتتالية ويجب أن نكون على حذر لا يجب أن يكون هناك تفريق ما بين الاصفر ، و يجب أن نعلم انا هذه القاعدة تقول إذا وجدة خانة كلها اصفار نستطيع أن نقوم بحذف جميع الاصفر و ترك صفر واحد هو الذي يمثل الخانة كما في المثال التالي.

2005:0005:0100:0:0:0:0:070

- لاحظ إنه تم تصغير العناوين ، و نستطيع ايضاً اختصار باقي الاصفر التي تبداء من جهة اليسار بمعنى إنه يوجد خانة فيها **0005** هذه الخانة نسطيع أن نقوم بحذف الاصفر الموجودة فيها بكل سهولة ليصبح شكل العنوان كما في المثال التالي :

2005:5:100:0:0:0:0:70

- الأن بعد الوصول لهذه المرحلة في عملية الاختصار تتبقى لدينا قاعدة واحدة ، و هي لو لاحظة في العنوان اعلى إنه يوجد اربعة اصفر في كل خانة لوحده اربعة اصفر ، و نستطيع اختصار هذه الاصفار بعملة الـ **:: Colon** مرتين ليصبح شكل العنوان كتالي:

2005:5:100::70

ملاحظة مهم جداً : لا يجب أن يكون **4 Colon** في العناوين السادس بعد عملية الاختصار ، و يعتبر خطاء في العنوان مثل التالي **2005:5::100::70** لاحظ إنه يوجد اربعة **Colon** بهذا الشكل يكون العنوان خطاء ولا نستطيع أن نعمل فيه .

أنواع العناوين المنطقية الخاصة IPv6

العناوين المنطقية الخاصة Private IPv6 Address

١- APIPA = Link-Local Unicast Address

الـ **APIPA** كانت تسمى في عنوان الإصدار الرابع ، ولكن تم تغير اسمها في عنوان الإصدار السادس ليكون **Link-Local Unicast Address**.

٢- Private IP Address = Unique-Local Address.

في الإصدار الرابع كان يسمى Private IP Address ، وتم تغير اسمها في الإصدار السادس ليكون **Unique-Local Address.**

٣- Public IP Address = Global Unicast Address

العناوين العامة التي يقوم بتوزيعها مزودي خدمة الإنترنت كان تسمى في الإصدار الرابع **Public IP Address** و تمى تغير اسمها في الإصدار السادس الـى **Global Unicast.**

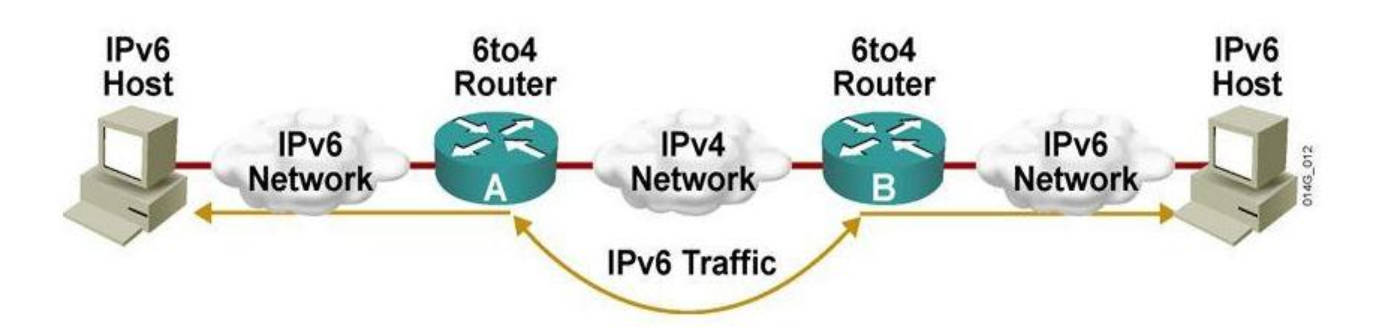
٤- ff02::1 Multicast Address

عنوان البث المتعدد كان في الإصدار الرابع **224.0.0.0** و تم تغيره في الإصدار السادس الى **ff02::1** .

٥- 127.0.0.1 = ::1 Loopback interface

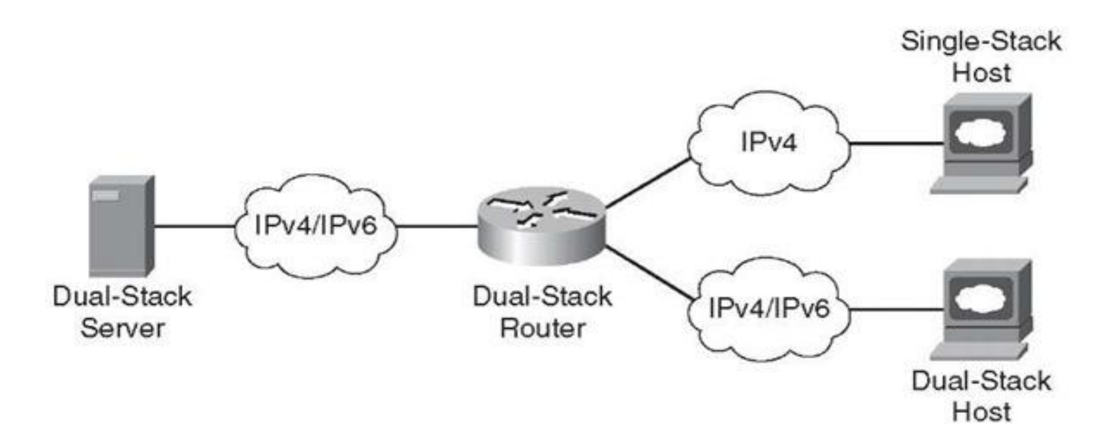
Loopback interface الذي يكون على كرت الشبكة كان في الإصدار الرابع **127.0.0.1** و تم تغيره في الإصدار السادس الى **:1** .

الأن بعد أن تعرفنا على أهم المميزات في اصدار العنوان السادس، يوجد نقطة مهم جداً جداً و هي عملية التحويل ما بين الإصدار الرابع **IPv4** و الإصدار السادس **IPv6** والربط بينهما و تسمى هذه الخاصية **Transition IPv4 to IPv6 ,** و يندرج تحت هذه الخاصية ثلاث تقنية تعمل على عملية التحويل سأقوم بذكرها و شرحها



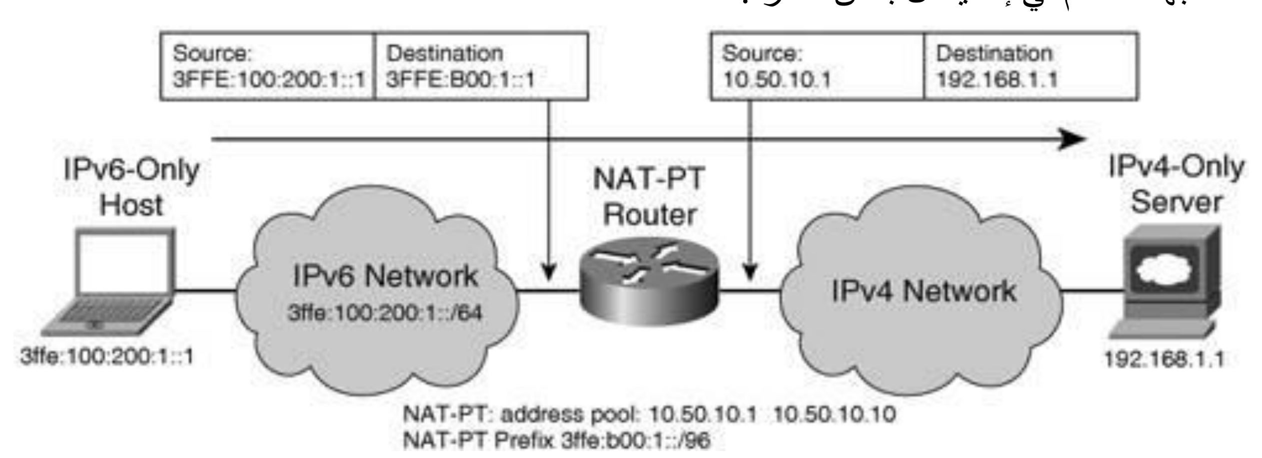
- تقنية الربط ما بين IPv4 و IPv6 :

١- **Dual Stack :** هذه التقنية المسؤولة عن الربط ما بين الإصدار الرابع **IPv4** و الإصدار السادس **IPv6** ، وتبدأء هذه العملية بعد أن نقوم بعمل إعدادات للمنفذ المراد أن يعمل مع الإصدار أن من العناوين الإصدار الرابع و الإصدار السادس، حيث إنه يقوم المنفذ بإرسال البيانات التي تعمل مع الإصدار الرابع **IPv4** و يعمل ايضاً على إرسال البيانات التي تعمل مع الإصدار السادس **IPv6** من دون اية تعارض كما في النموذج التالي .

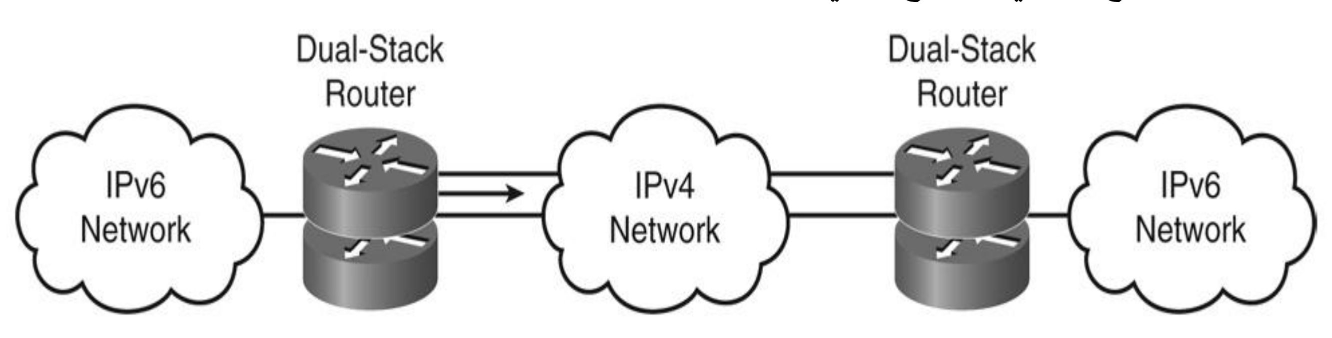


٢- **NAT Protocol Translation (NAT-PT) :** هذه التقنية تعمل على الراوتر حيث إنه تقوم بعملية التحويل ما بين العناوين مختلفة الإصدار ات ، مثل عندما يتوجد لدنيا شبكة تعمل بعنوان الإصدار الرابع **IPv4** و شبكة تعمل بعنوان الإصدار السادس **IPv6** و عندما يريد أحد الأجهزة الموجودة في الشبكة التي تعمل بعنوان الإصدار الرابع ، يريد أن يرسل بيانات لشبكة اخرى تعمل بعنوان الإصدار السادس ستقوم البيانات بذهاب الى الراوتر حيث يقوم الراوتر بعملية الترجمة من الإصدار الرابع الى الإصدار السادس و العكس و يقوم بإرسال ه للشبكة الآخر كما في النموذج التالي.

ملاحظة مهم جداً : يجب أن لا نخلط ما بين بروتوكول الـ **NAT** الذي كان يعمل مع عنوان الإصدار الرابع حيث إنه يختلف اختلف كامل عن تقنية الـ **NAT-PT** ، ولكن تم تسميته بهذا الاسم لي إنه يعمل بنفس الفكره.



٣- **IPv6 Over IPv4 Tunels :** هذه التقنية مهم جداً و تلزم عندما ا يكون لدينا أكثر من شبكة تعمل مع عنوان الإصدار السادس **IPv6** ، و نريد أن نربط هذه الشبكة التي تعمل مع عنوان الإصدار السادس في بعضها البعض سنحتاج شبكة في المنتصف لتقوم بربط هذه الشبكة في بعضهم البعض و ستكون هذه الشبكة تعمل بعنوان الإصدار الرابع **IPv4** و من خلال هذه الشبكة ستقوم جميع الشبكات التي تعمل في عنوان الإصدار السادس أن تستطيع الاتصال في بعضها البعض ، بعد أن نقوم من تفعيل و اعداد هذه التقنية على الراوترات الموجودة في الشبكة التي في المنتصف و تعمل بعنوان الإصدار الرابع كما في النموذج التالي .



IPv4 Header / IPv6 Header

- بروتوكول الـ **IP** يتكون من **Header** و في داخل هذا الـ **Header** يتوجد عدة خانات ، كل خانة له وظيفه محددة حيث يتم بناء الـ **Header** من اعلى الى اسفل بشكل مرتب بعد أن يقوم بإضافة المعلومات و البيانات المطلوبة والتي يجب أن يتم اضافته في كل خانة من الخانة ، سأقوم بشرح هذه الخانة بالتفصيل الممل و نستعرف على كل خانة ما هي وظيفته و على ماذا تحتوي ، و يجب أن نعلم إنه كما ذكراً سابقاً يوجد نوعان من العناوين عنوان من الإصدار الرابع و عنوان من الإصدار السادس و كل من هذه العناوين تحتوي على **Header** خاص بكل عنوان ، و مع العلم إنه يوجد بعض التغيرات ما بين الـ **IPv4 Header** و **IPv6 Header** سأقوم بشرح كل واحد بشكل منفرد لنتعرف عليهم بشكل ممتاز .

قبل أن نبداء في الشرح يجب أن نتعرف على حجم و طول كل من الـ **IPv4 Header** و **IPv6 Header** لنكون على معرفة في كل شيء .

IPv4 Header: حجمه **32 byte**، و طوله **20 byte**.

IPv6 Header: حجمه **32 byte**، و طوله **40 byte**.

كما في النماذج التالية :

IPv4 Header / IPv6 Header

IPv4 Header

Version | IHL | Type of Service | Total Length
Identification | Flags | Fragment Offset
Time to Live | Protocol | Header Checksum
Source Address
Destination Address
Options | Padding

IPv6 Header

Version | Traffic Class | Flow Label
Payload Length | Next Header | Hop Limit
Source Address
Destination Address

Legend

- Field's Name Kept from IPv4 to IPv6
- Fields Not Kept in IPv6
- Name and Position Changed in IPv6
- New Field in IPv6

- الأن سنبداء بتعرف على **IPv4 Header** سنتعرف على جميع الخانات الموجودة في داخله ، و بعدها سنتعرف على **IPv6 Header** .

- الخانات الموجودة في **IPv4 Header** عددهم **14** خانة سأقوم بذكرهم و شرحهم .

Version , IHL , Type of Service , Total Length , Identification , Flags , Fregment Offset , Time to live , Protocol , Header Checksum , Source Address , Destination Address , Options , Padding .

- هذه هي الخانات الموجودة في عنوان الإصدار الرابع كما هي موجودة في النموذج اعلى و سأقوم الأن بشرح كل واحدة .

- **النسخة Version:** هذه الخانة المسؤولة عن ترويسة البروتوكول الخاص في الإنترنت ، حيث تقوم بتحديد رقم الصيغة و رقم نسخة أو اصدار البروتوكول طبعاً الـ **IPv4** ليستطيع المستقبل فهم الية التعامل مع الـ **Header** و أجزاءه و خاناته ، و حجم هذه الخانة **4 bit**.

- **IHL:** وظيفة هذه الخانة إنه تقوم بعملية ترويس لبروتوكول الـ **IP** ليكون بحجم **32 bit** ، حيث يدل على بداية جمع المعلومات و حجم هذه الخانة **4 bit** .

- **Type of Service :** هذه الخانة المسؤولة عن تحديد نوع الخدمات المطولبة ، مثل خدمة نقل المعلومات و البيانات التي يرساله المستخدمين و معلومات التوجيه و الكثير من الخدامات الآخر و حجم هذه الخانة **8 bit** .

- **Total Length** : هذه الخانة هي المسؤولة عن تحديد طول الرسالة أو بمعنى آخر طول حزمة البيانات و بعده يقوم بإضافة طول الترويسية و حجم هذه الخانة **16 bit**.

- **Identification** : هذه الخانة المسؤولة عن اعادة تجميع الحزم كما كانت من بداية تجميعها و تستخدم ايضاً لتميز الحزم عن بعضهم البعض ، وحجم هذه الخانة **16 bit** .

- **Flags** : هذه الخانة هي المسؤولة عن تقنية الاتصال مثل تقوم بعملية تحديد لحزمة البيانات المستقبلة هل هي آخر حزمة من البيانات أو لا و حجم هذه الخانة **3 bit** .

- **Fregment Offset** : هذه الخانة من أهم الخانات الموجودة و وظيفة هذه الخانة إنه تقوم بعملية تجزئة للحزمة المرسلة إذا كانت كبيرة ، بمعنى كبيرة إذا كانت اكبر من الحجم المسموح به في داخل الشبكة و حجم هذه الخانة **13 bit** .

- **Time to live** : هذه الخانة المخصصة لعملية الوقت مثل عندما ترسل الحزمة يجب أن نعلم أن في داخل الحزمة يوجد عدة بيانات أو خصائص ، حيث يتم تحديد وقت معين لهذه الحزمة ولكن في حال بقة هذه الحزمة تدور في شبكة الايثرنيت لفترة اطول من الازم أو قد تم اجتياز الوقت المحدد لهذه الحزمة ، دون أن تصل للهدف المطولب ستتوقف الحزمة عن عملية الإرسال و ستقوم بالغاء العملية بنفسها و حجم هذه الخانة **8 bit** .

- **Protocol** : هذه الخانة المسؤولة عن البروتوكولات التي سيتم استخدامها في جزء من البيانات المرسلة في داخل الحزمة و حجم هذه الخانة **8 bit** .

- **Header Checksum** : تستخدم هذه الخانة في عملية التاكد من سلامة البيانات في اقسام تجميع البيانات ما قبل إرسال ه حيث تقوم هذه الخانة ببعض العملية الحسابية و حساب نتيجتها و إذا تاكد من إنه صحيح سيتم إرسال ، و عند وصول الرسالة للهدف المطلوب سيتم إعادة حساب القيمة مرة أخرى فإذا تطابقت القيمتان سيتم التاكد من من سلامة النقل .

- **Source Address :** هذه الخانة المسؤولة عن عنوان الـ **IP** لجهاز المرسل ، وحجم هذه الخانة **32 bit** .

- **Destination Address :** هذه الخانة المسؤولة عن عنوان الـ **IP** لجهاز المستقبل ، وحجم هذه الخانة **32 bit** .

- **Options:** هذه الخانة تستخدم في عملية الخيارات مثل وظائف التحكم في الاتصالات مثل الامن و التوجيه و المسارات هذه غير ضرورية، ويبدا حجم هذه الخانة من **0** الى **32**.

- **Padding أو Data:** هذه الخانة هي من أهم الخانة التي قمنا بذكرها و وظيفة هذه الخانة إنه تحتوي على جميع البيانات التي قمنا بذكرها و التي سيتم إرسال ه، هذه الخانة لا يوجد له حجم محدد بينما تاخذ حجمه عندما ا تكتمل البيانات كلها و مع العلم إنه البيانات متغيرات بمعنى إنه لا يوجد له حجم حدد و هذه الخانة هي المعتمد عليها من جميع الخانة التي ذكرنها مسبقاً.

IPv6 Header

IPv6 Header: قبل أن نبداء في التعرف على الإصدار السادس يجب أن نتذكر إنه الـ **IPv4 Header** يتكون من **14** خانة، و تم اختصار **8** خانات في الإصدار السادس ليصبح **8** خانة سأقوم بذكرهم مع العلم إنهم نفس الحقول ولكن يوجد بعض الاختلف .

- **النسخة Version:** هذه الخانة المسؤولة عن ترويسة البروتوكول الخاص في الإنترنت ، حيث تقوم بتحديد رقم الصيغة و رقم نسخة أو اصدار البروتوكول طبعاً الـ **IPv6** ليستطيع المستقبل فهم الية التعامل مع الـ **Header** و أجزاءه و خاناته ، و حجم هذه الخانة **4 bit**.

- **Traffic Class :** هذه الخانة نفسه خانة الـ **Type of Service** ولكن تم تغيره اسمها في الإصدار السادس لتكون **Traffic Class**.

- **Flow Label :** هذه خانة جديد تم اضافتها في الإصدار السادس ولم تكن موجودة في الإصدار الرابع ، و هي الخانة المسؤولة عن تحديد تدفق البكت و تستخدم ايضاً مع جودة الخدمة .

- **Payload Length :** هذه الخانة نفسه خانة الـ **Total Length** في الإصدار الرابع و تم تغيره لـ **Payload Length** في الإصدار السادس .

- **Next Header :** هذه الخانة نفسه الـ **Protocol** في الإصدار الرابع و تم تغيره لـ **Next Header** في الإصدار السادس .

- **Hop Limit :** هذه الخانة هي نفسه **Time to live** في الإصدار الرابع و تم تغيره لـ **Hop Limit** في الإصدار السادس .

- **Source Address :** هذه الخانة المسؤولة عن عنوان الـ **IP** الخاص في جهاز المرسل و يكون حجم عنوان الإصدار السادس في هذه الخانة **128 bit** بينما في هذا الحقل في الإصدار الرابع يكون حجم العناون **32 bit** ، و حجم هذه الخانة على حجم العنوان **128 bit** .

- **Destination Address :** هذه الخانة المسؤولة عن عنوان الـ **IP** الخاص في جهاز المستقبل ويكون ايضاً عنوان من الإصدار السادس و يكون حجم هذه الخانة **128 bit** كما هي في خانة المرسل ، و حجم الخانة سيكون ايضاً **128 bit** على حجم العنوان .

- الخانات التي تم حذفها من الإصدار السادس: **Checksum, Option, Fragmentatio**

فهرس المستوى الثاني

Routing Networks التوجيه في الشبكات

جهاز الراوتر أو الموجه

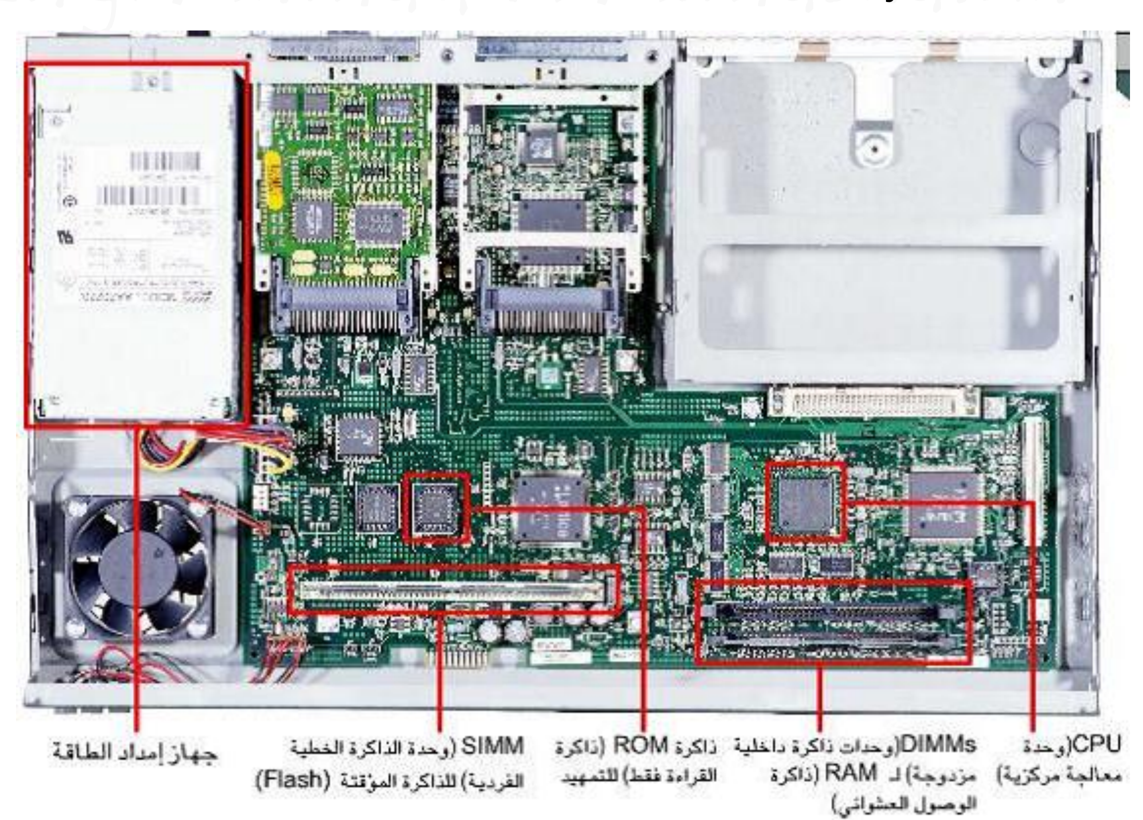
Devices Router

- جهاز الراوتر أو الموجه هو الجهاز المسؤولة عن ادارة و ربط الشبكات المختلفة عن بعض .

المكونات الخاصة في جهاز الراوتر أو الموجه - **Router Components :**

١- المعالج
٢- الذاكرة
٣- ذاكرة الوصول العشوائية
٤- ذاكرة القراءة فقط
٥- ذاكرة الفلاش
٦- الذاكرة الغير قابلة للحذف

1- CPU = Central Processing Unit
2- Memories
3- RAM = Random – access memory
4- ROM = Read-Only memory
5- Flash Memory
6- NVRAM = Non – Volatile Random – access memory



صورة الراوتر من الداخل

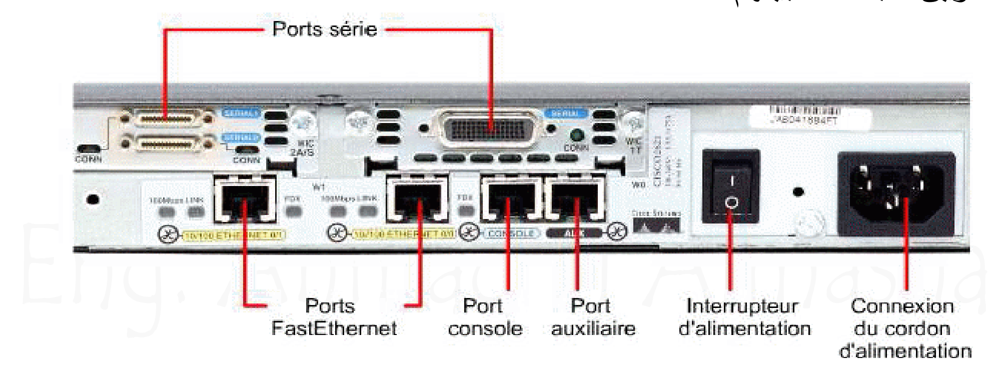
المنافذ Interface :

١- **Console Port:** هذا المنفذ المختص في عمل الاعداد الخاص في جهاز الراوتر يتم ربط كابل يسمى **Console** في هذا المنفذ و بعد ذالك يتم الربط من الطرف الآخر في جهاز الكمبيوتر لنستطيع الدخول على الراوتر و عمل الاعدادة و برمجة الراوتر هذا المنفذ يتوجد على جهاز السويتش ايضاً.

٢- **Auxiliary Port:** هذا المنفذ يتم أستخدامه لعمل اعدادة الجهاز ايضاً ولكن عن بعد بمعنى يجب أن يكون الراوتر متوصل على شبكة الإنترنت ليتم الدخول عليه و عمل الإعدادات عن بعد من مكان اخرى.

٣- **LAN Interfaces:** هذا المنفذ مخصص للشبكات الداخلية فقط يستخدم لربط الشبكات المختلفة في بعضها البعض القريب بمعنى داخل حدود الشركة.

٤- **WAN Interfaces:** هذا المنفذ مخصص لربط الشبكات في بعضها البعض التي تكون ما بين الدول و البعيدة و يستخدم ايضاً لربط فروع الشركات في بعض لتتمكن من تكوين شبكة ما بينهم.



منافذ الراوتر

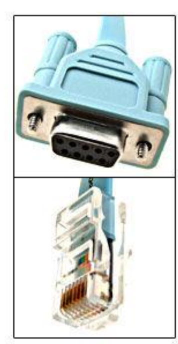
الكابلات التي يتم تركيبها في منفذ الـ Port Serial :

١- **DCE = Data Communication Equipment**

٢- **DTE = Data Terminal Equipment**

كابل السيريل : يستخدم هذا الكيبل للربط بين الفروع أو الراوترات المحتوية على كروت السيريال حيث يسمى احد الطرفين (**DCE**) والطرف الآخر (**DTE**) و احيانا يتم ربط الراوتر بجهاز الفريم ريلاي سويتش مثل (**Cisco 2522**) عن طريق نفس الكيبل . كيبلات (**DCE/DTE**) تستخدم بشكل اساسي في معامل سيسكو





تسلسل إقلاع الراوتر الخاص في سيسكو

Cisco Router Boot Sequence

نظام البوت للإقلاع : هو مجموعة من الخطوات المتسلسلة التي تقوم بها الأجهزة بشكل عام و التي تحتوي على نظام تشغيل بإتباعها لكي يعمل و تبدا بفحص القطع المادية للجهاز تحديد قرص التخزين أو الذاكرة التي سوف يتم إقلاع الجهاز منها و تحميل نظام التشغيل و الإعدادات و يعمل الجهاز و في كل مرة يتم تشغيل الجهاز فإنه يقوم بإتباع نفس الخطوات للنظام التسلسلي للإقلاع .

- **شرح عملية تسلسل إقلاع الراوتر Boot Sequence :**

١- تشغيل الفحص الذاتي **Post = Power on self-Test**

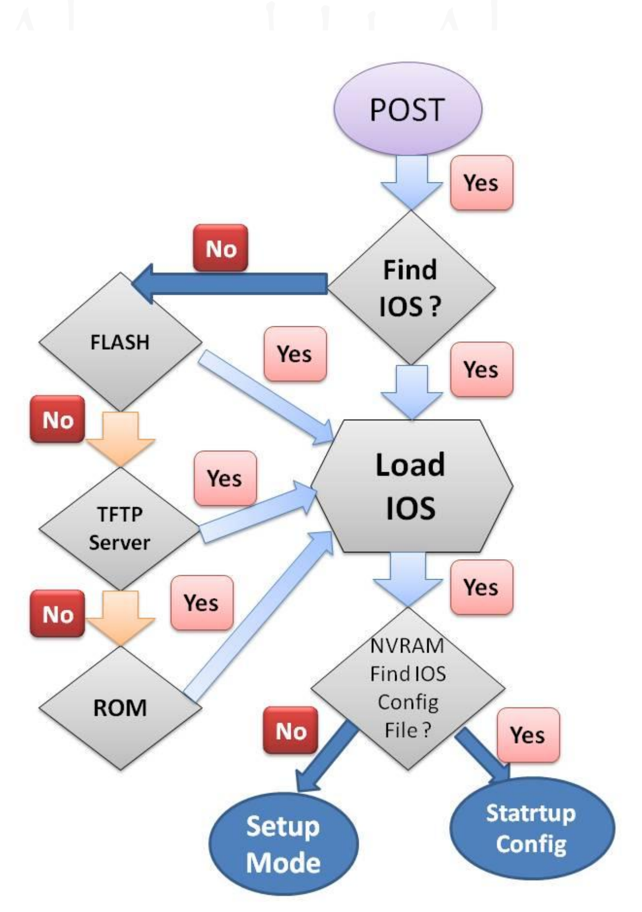
٢- تشغيل الـ **Boot Strap**

٣- البحث عن نظام تشغيل **ISO = Internetwork OS**

٤- تحميل نظام التشغيل من ذاكرة الفلاش و إرسالـه إلى الرام **RAM**

٥- البحث عن ملف الإعدادات **Startup – Configuration**

٦- تحميل ملف الإعدادات من ذاكرة الـ **NVRAM** إلى ذاكرة الـ **RAM** و بالتي سيتم تشغيل ملف الإعدادات **Running Configuration** و بعده سيتم تشغيل الراوتر بشكل صحيح .



مستويات سيسكو في برمجة الأجهزة

Cisco Modes Devices

شركة سيسكو تقوم بعمل مستويات في عملية إعدادات الأجهزة مثل الراوتر أو السويتش و تتكون هذه المستويات من ثلاث مستويات :

١- المستويات الأساسية. ٢- المستويات الفرعية. ٣- المستويات الفرعية .

١- المستويات الأساسية

مستوى المستخدم User Exec Mode

Router >

مستوى الوصول Privilege Exec Mode

Router > Enable

Router #

مستوى الإعدادات Global Configuration Mode

Router # Config Terminal

Router (config) #

٢- المستويات الفرعية

مستوى إعدادات المنفذ Interface Configuration Mode

Router (config) # interface fast Ethernet 0/1

Router (config-if) #

مستوى إعدادات المنفذ الفرعي (الافتراضية) Sub Interface Configuration Mode

Router (config) # interface fast Ethernet 0/1.1

Router (config-subif) #

مستوى إعدادات بروتوكولات التوجيه Routing Protocol Mode

Router (config) # router eigrp 1

Router (config-router) #

٣ـ المستوى المستقلة

مستوى الإعدادات الاساسية Setup Mode

Continue with configuration dialog? [Yes/no]:

Rommon Mode

Rommon 1 >

أنظمة تشغيل سيسكو

Cisco IOS

شركة سيسكو تقوم ببرمجة أنظمة التشغيل و التي تعمل في أجهزة سيسكو المختلفة مثل الراوترات و السويتش ات و الفايرول و غيره من الأجهزة الخاصة في شركة سيسكو و هي تعمل بنظام الاوامر النصية و يتواجد لدنيا اربعة أنظمة تشغيل سأقوم بشرحهم :

IOS: هو نظام تشغيل يعمل مع الأجهزة التي تحتوي على معالج واحد.

IOS XE: هو يعتبر تطوير لنظام الـ **IOS** حيث يحتوي على مجموعة من الخصائص المتقدمة مثل فصل عملية الإرسال عن عملية التحكم كذلك يعدم وجود اكثر من معالج في جهاز سسيكو.

IOS-XR: هو نظام يعمل في أجهزة سيسكو صاحبة المواصفات العالية و غالباً ما تتواجد في شبكات الاتصالات.

NX-OS: هو نظام يعمل في أجهزة سيسكو التي تعمل في شبكات مراكز البيانات.



Basic Command

Router

Router > **?**	All Command
Router > **enable**	To get to Privileged Mode
Router # **disable**	To get back to User Mode
Router > **terminal history size**	To set the command buffer size
Router > **terminal no editing**	To disable advanced editing features
Router > **show history**	To show the command buffer
Router # **config t**	Enter global configuration mode
Router # **show version**	View IOS version
Router # **show interface**	Display interfaces on router and their status
Router # **show ip interface brief**	Check interface status
Router # **show ip protocol**	Display ip protocol info
Router # **show protocol**	Display which protocols are configured on the router
Router # **show flash**	View IOS version, size of IOS, and free space in FLASH
Router # **show running-config**	View current configuration file (RAM)
Router # **show startup-config**	View saved configuration file (NVRAM)
Router # **show processes cpu**	View CPU utilization
Router # **show processes**	View info about programs in RAM
Router # **reload**	Reboot the router and reload the startup config from NVRAM
Router(config) # **no ip routing**	Disable IP routing on a router (enabled by default)
Router(config)# hostname Router1	Give the router a hostname
Ctrl+**A**	To move to the beginning of the command line

Ctrl+**E**	To move to the end of the command line
Ctrl+**F**	To move forward one character
Ctrl+**B**	To move back one character
Ctrl+**W**	To move forward one word
Ctrl+**U**	To erase a line
Ctrl+**R**	To redisplay a line
Router # Ctrl+**Z**	Ends configuration mode and returns to privileged mode
Router # **show ip route**	View the IP routing table
Router # **debug ip rip**	View RIP Debug
Router # **debug ip igrp events**	View IGRP Debug
Router(config) # **no router rip**	Disable RIP routing
Router # **copy flash tftp**	Backup IOS to file server
Router#**copy tftp flash**	Upgrade the IOS from the file server
Router # **copy running-config tftp**	Copy running config file from RAM to TFTP
Router # **copy tftp running-config**	Copy startup config file from TFTP to RAM
Router # **copy tftp startup-config**	Copy startup config file from TFTP to NVRAM
Router # **erase startup-config**	Erase the configuration file in NVRAM [run initial config dialog]
Router(config)# **boot system flash (ios_filename)**	Tell router which IOS file in Flash to boot from
Router(config) # **boot system tftp (ios_filename) tftp_ip_address**	Tell router which IOS to request from the TFTP server (fallback)
Router(config) # **boot rom**	Tell router to boot from IOS in ROM
Routerconfig) # **service password-encryption**	Passwords can be encrypted
Routerconfig) # **no service password-encryption**	To de-encrypt the passwords

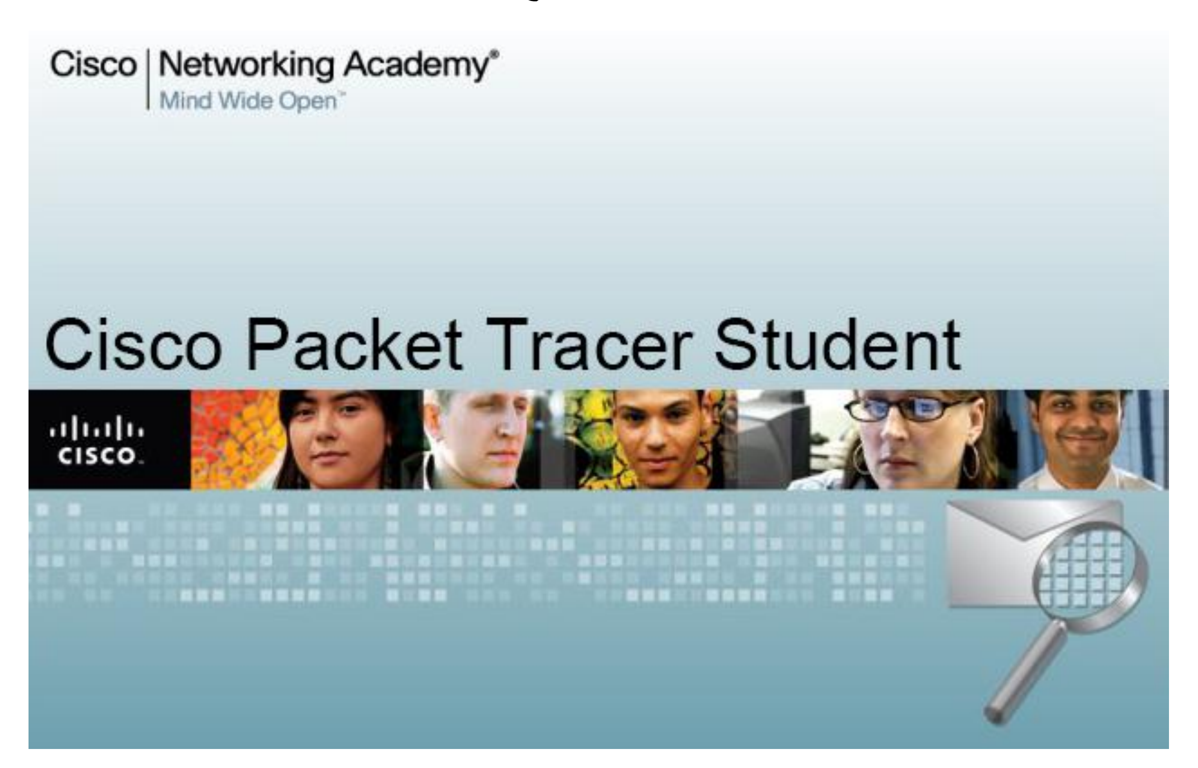
الجزء العملي

Install packet tracer

الجزء العملي من الكتب و قبل أن نبداء في هذا الجزء من التطبيق بشكل عملي يجب معرفة إنه يوجد برنامج من شركة سيسكو مجاني و هذا يساعد الطالب على التدريب العملي و يجعلك تتمرن بشكل ممتاز على الاوامر و الأجهزة و تصميم الشبكات .

برنامج Packet Tracer : هو برنامج محاكاة لشبكات الحاسوب , كما يمكن تصميم الشبكات كما نريد و فائدة هذا البرنامج يجعلك أن تقوم بتصميم شبكة كاملة مكملة قبل بناء الشبكة على أرض الواقع و عمل اختبار للشبكات و معرفة كيف سيتم بناء الشبكة على أرض الواقع.

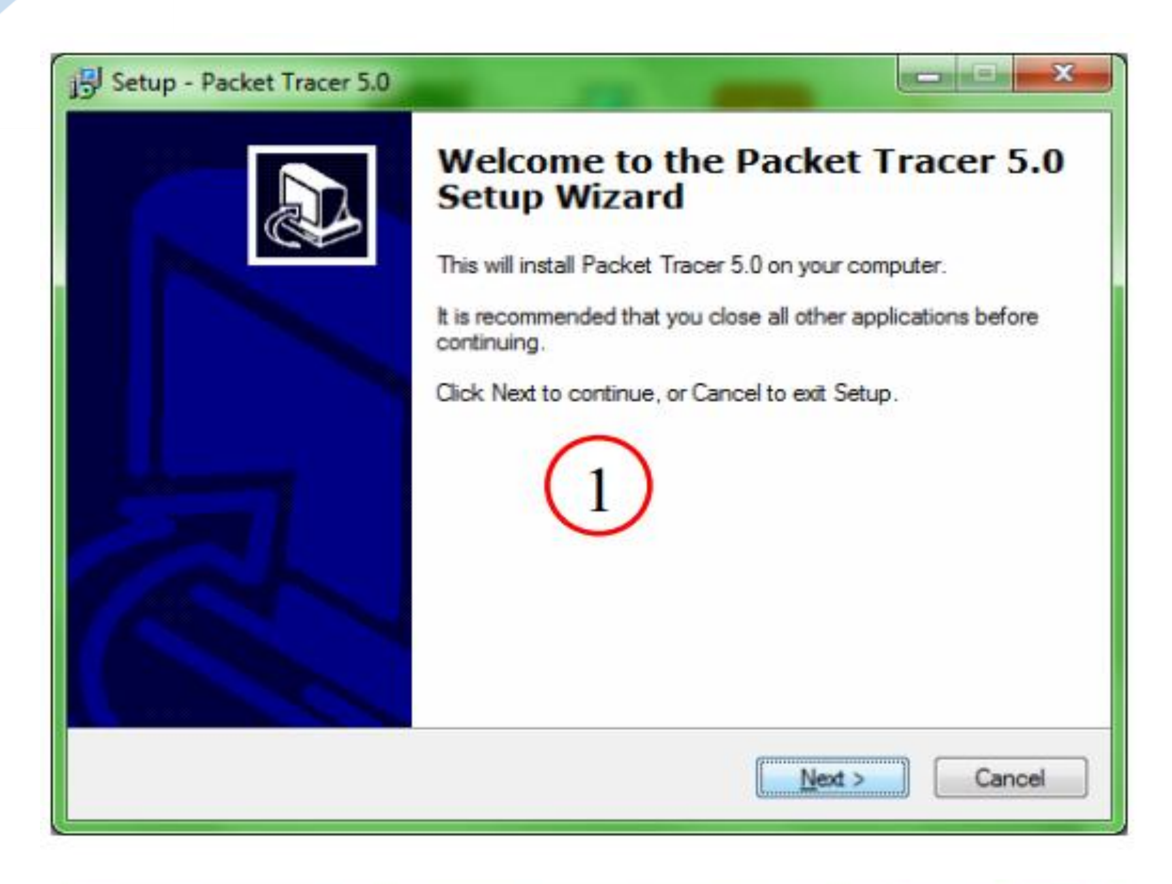
صورة البرنامج

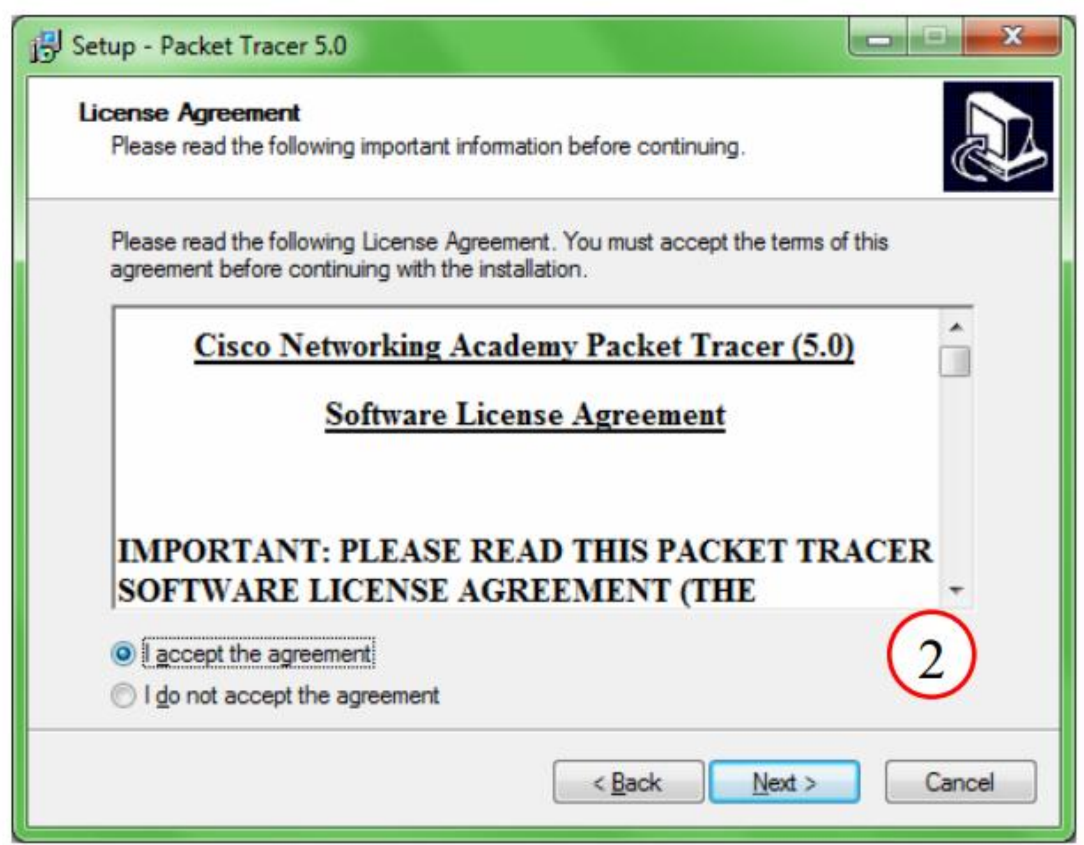


خطوات تثبيت البرنامج ......

١- بعد ما قمنا بالنقر المزدوج على أيقونة البرنامج فستظهر لنا شاشة التثبيت نضغط على **Next** .
٢- ثم ننتظر لحظات لتظهر لنا شاشة جديدة نختار الخيار المؤشر إليه ثم نضغط **Next**.
٣- نبقى نضغط **Next** حتى تظهر شاشة ذات **Install** .
٤- ستظهر لنا شاشة تفيد حالة التثبيت و تقدمه .
٥- ستظهر لنا رسالة بعد إتمام التثبيت تفيد بأن التثبيت قد انتهى قم بضغط على **Finish**.

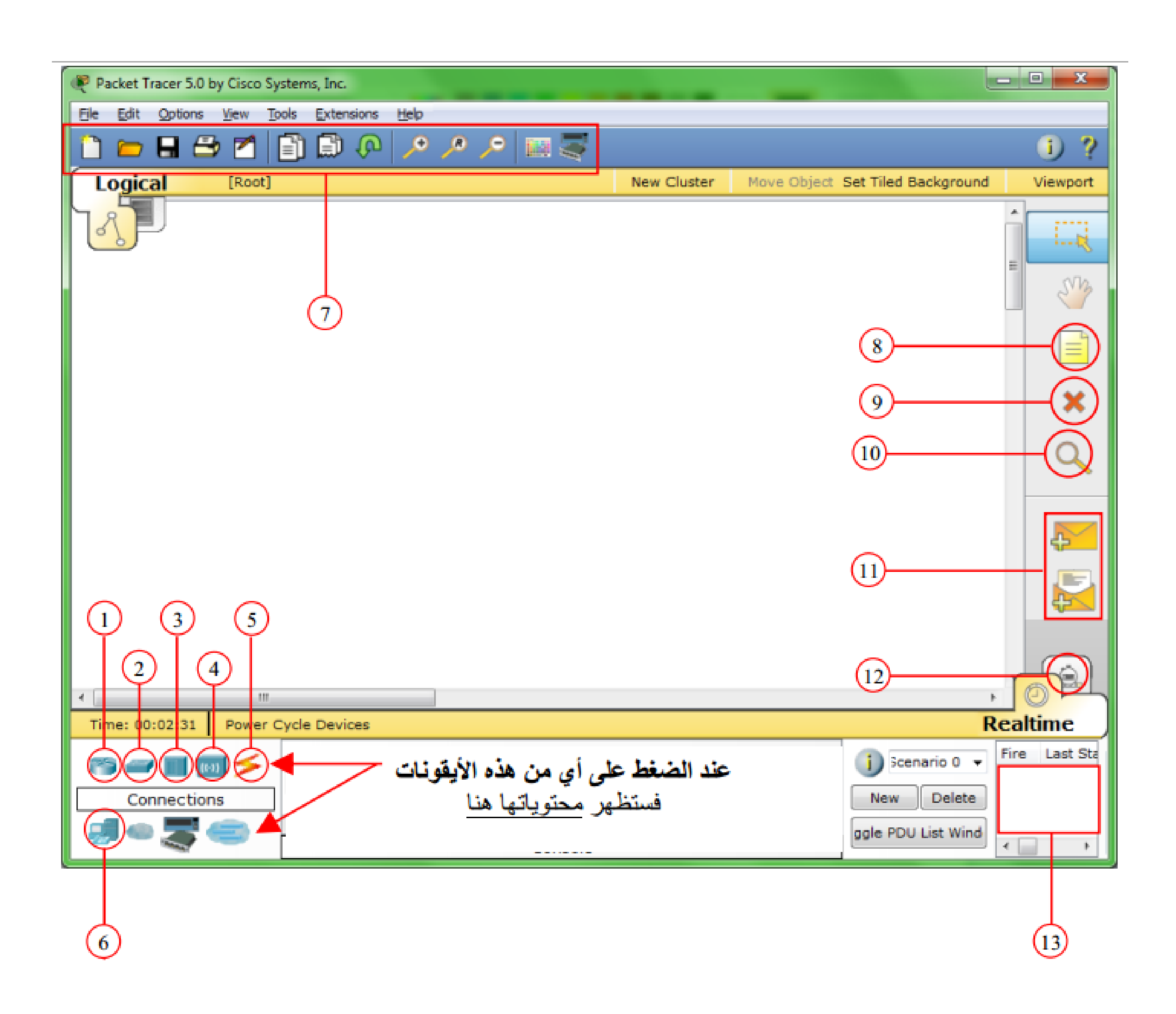
رابط تحميل البرنامج https://www.itechtics.com/download-cisco-packet-tracer-6-2-free-direct-download-link/


Setup - Packet Tracer 5.0
Welcome to the Packet Tracer 5.0 Setup Wizard
This will install Packet Tracer 5.0 on your computer.
It is recommended that you close all other applications before continuing.
Click Next to continue, or Cancel to exit Setup.
1
Next >
Cancel


Setup - Packet Tracer 5.0
License Agreement
Please read the following important information before continuing.
Please read the following License Agreement. You must accept the terms of this agreement before continuing with the installation.
Cisco Networking Academy Packet Tracer (5.0)
Software License Agreement
IMPORTANT: PLEASE READ THIS PACKET TRACER SOFTWARE LICENSE AGREEMENT (THE
I accept the agreement
I do not accept the agreement
2
< Back
Next >
Cancel

التعرف على محتويات البرنامج :

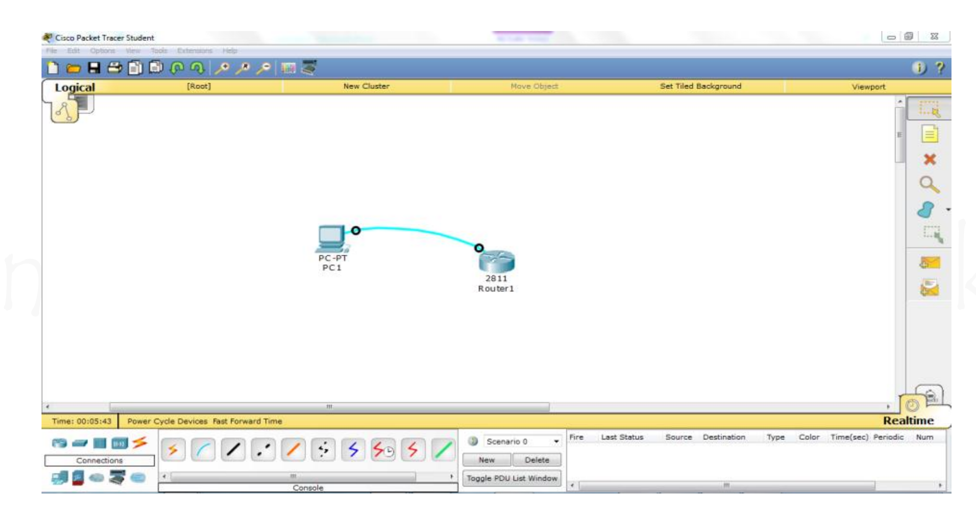
١- Router
٢- Switches
٣- Hubs
٤- Wireless Devices
٥- Connection
٦- End Devices
٧- أوامر للوصل السريع
٨- لكتابة
٩- للحذف نضغط على الأداة أولا ثم نضغط على المراد حذفه
١٠- لمعرفة بيانات الخاصة بالرسائل
١١- رسائل
١٢- لمعرفة كيفية تنقل الرسائل عبر الشبكة و كيف ترسل
١٣- بيانات متعلقة بالرسائل ومن خلالها يمكن تحرير أو حذف الرسالة



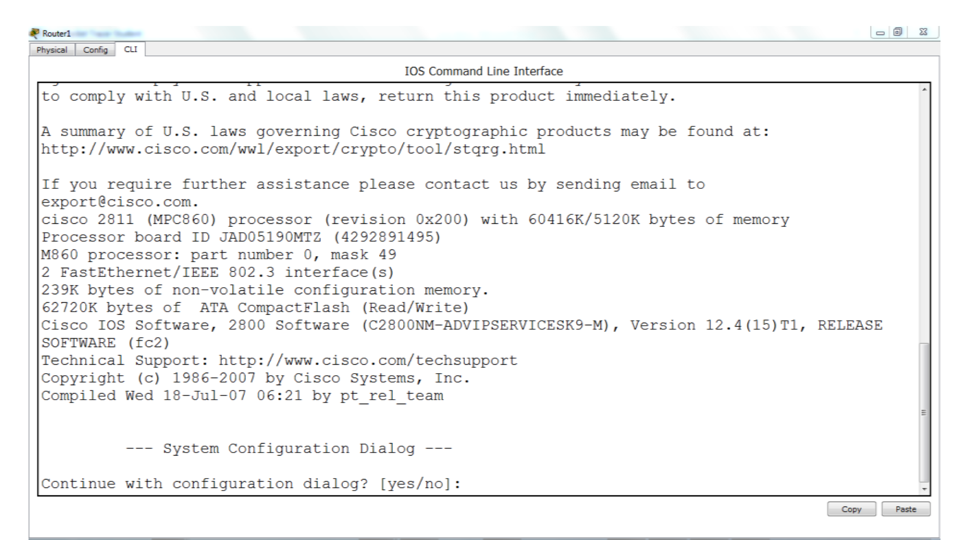
Router Passwords
And Password Recovery

- **شرح تأمين نقاط الدخول لجهاز الراوتر أو السويتش :**

- قبل البداء في عملية التأمين يجب التذكر إنه يوجد أكثر من منفذ على الجهاز مثل جهاز الراوتر يوجد عليه منفذ الأعدادات و منفذ التحكم عن بعد الأن عندما نريد تأمين هذه المنافذ يجب علينا أن نبداء في تأمين المنفذ الأول و هو منفذ الإعدادات **Console** لإنه هو المنفذ الرئيسي الذي سيتم منه الدخول للجهاز .
- نبداء في العمل الأن هذه الصورة يوجد فيها جهاز راوتر و يوجد فيها ايضاً جهاز حاسوب تم توصيل جهاز الراوتر بجهاز الحاسوب عن طريق كابل الـ **Console** الأن سأقوم بدخول على إعدادات الراوتر و البداء في عملية تأمين نقاط الدخول سأقوم بشرح كل نقطة من البداية للنهاية .



الأن متوجدين في داخل الراوتر



سنقوم بكتابة No و الدخول للتالي :

Router1

Physical | Config | CLI

IOS Command Line Interface

```
cisco 2811 (MPC860) processor (revision 0x200) with 60416K/5120K bytes of memory
Processor board ID JAD05190MTZ (4292891495)
M860 processor: part number 0, mask 49
2 FastEthernet/IEEE 802.3 interface(s)
239K bytes of non-volatile configuration memory.
62720K bytes of  ATA CompactFlash (Read/Write)
Cisco IOS Software, 2800 Software (C2800NM-ADVIPSERVICESK9-M), Version 12.4(15)T1, RELEASE
SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2007 by Cisco Systems, Inc.
Compiled Wed 18-Jul-07 06:21 by pt_rel_team


        --- System Configuration Dialog ---

Continue with configuration dialog? [yes/no]: no


Press RETURN to get started!



Router>
```

Copy | Paste

الأن سنقوم بكتابة التالي :

Router > **enable**

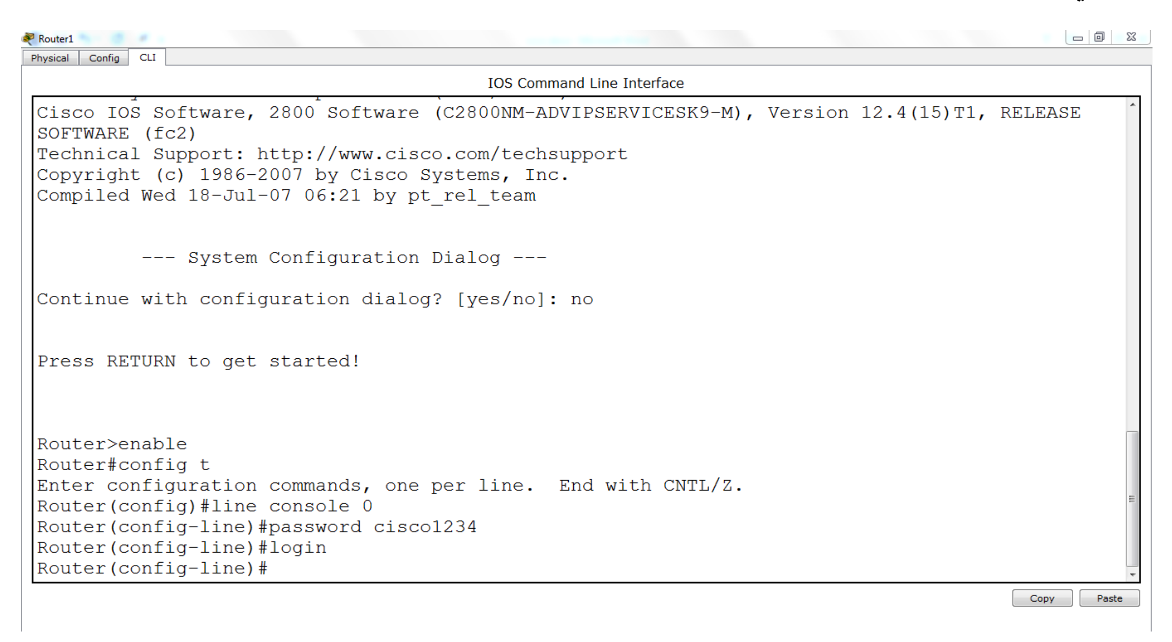
Router # **config t**

Router (config) # **line console 0** رقم صفر هذا رقم المنفذ الخاص في الإعدادات

Router (config-line) # **Password cisco123**

Router (config-line) # **login**

كما في الصورة التالية :



Router1

Physical | Config | CLI

IOS Command Line Interface

```
Cisco IOS Software, 2800 Software (C2800NM-ADVIPSERVICESK9-M), Version 12.4(15)T1, RELEASE
SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2007 by Cisco Systems, Inc.
Compiled Wed 18-Jul-07 06:21 by pt_rel_team


        --- System Configuration Dialog ---

Continue with configuration dialog? [yes/no]: no


Press RETURN to get started!

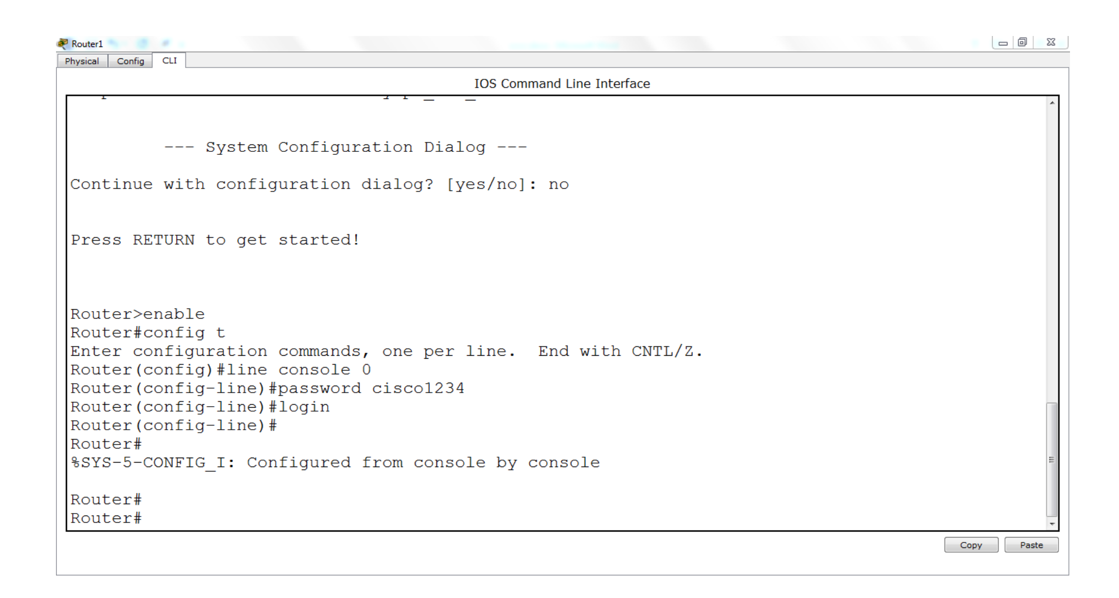


Router>enable
Router#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#line console 0
Router(config-line)#password cisco1234
Router(config-line)#login
Router(config-line)#
```

Copy | Paste

- الأن بهذه الطريقة تم تأمين المنفذ الأولى الخاص في الإعدادات **Port Console** .
- سنقوم بعملية الخروج من سطر الاوامر هذا و الإنتقال لمنفذ **Aux** للتحكم عند بعد .

- نقوم بضغط على **Ctrl + C** بهذه الطريقة سنعود للمستوى الأولى مستوى الإعدادات Router # كم هو واضح في الصورة التالية .



- **الأن سنقوم بتأمين منفذ التحكم عن بعد Aux :**

الأن سنقوم بكتابة التالي :

Router > **enable**

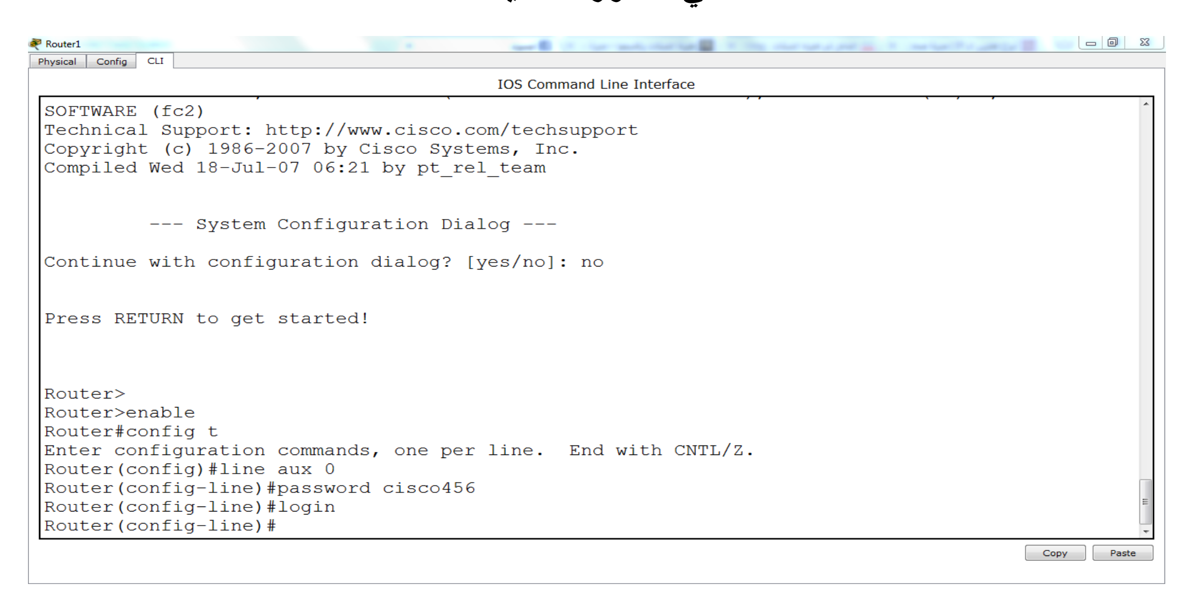
Router # **config t**

Router (config) # **line aux 0** رقم صفر هذا رقم المنفذ الخاص في الإعدادات

Router (config-line) # **Password cisco456**

Router (config-line) # **login**

كما في الصورة التالية :



- الأن بهذه الطريقة تم تأمين المنفذ الثاني الخاص في التحكم عن بعد **Port Aux** .
- سنقوم بعملية الخروج من سطر الاوامر هذا و الإنتقال لمستوى ثاني من عملية التأمين.

الأن سنقوم بتأمين مستوى الإعدادات و هو مستوى الـ Enable :

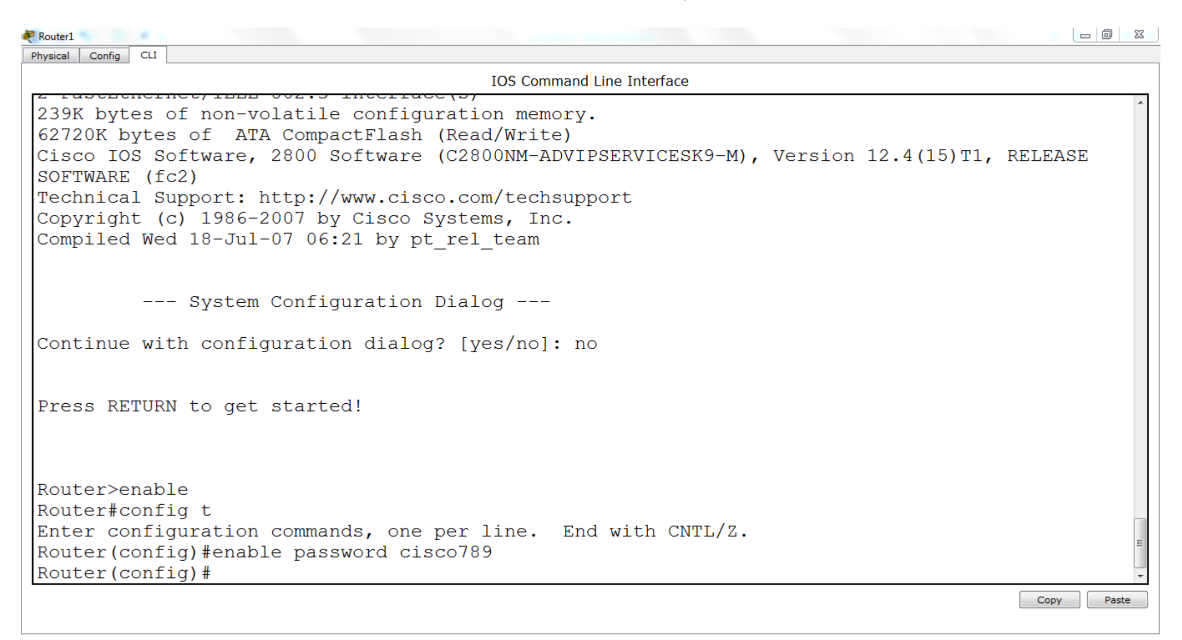
الأن سنقوم بكتابة التالي :

Router > **enable**

Router # **config t**

Router (config) # **enable password cisco789**

كما في الصورة التالية :



بعد هذا كله يجب أن نقوم بعملية التشفير الخاص في كلمة المرور :

الأن سنقوم بكتابة التالي :

Router > **enable**

Router # **config t**

Router (config) # **service password-encryption**

- الأن أمر التشفير هذا يقوم بتشفير كلمة المرور الخاصة في المنافذ لإنه لو تركنا كلمة المرور كما هي ستظهر بشكل التالي كم هو ظهرة بصورة التالية :

هذا هو الأمر يجب تفعيله مهم جداً Service password-encryption

- **ملاحظة مهم جداً :** هذا الأمر لا يدعم تشفير كلمة مرور مستوى الإعدادات .

هذه الصورة ما قبل عملية التشفير

```
Router1
Physical  Config  CLI
IOS Command Line Interface
ip flow-export version 9
!
!
!
!
!
!
!
line con 0
 password cisco123
 login
!
line aux 0
 password cisco456
 login
!
line vty 0 4
 login
!
!
!
end
Copy  Paste
```

عملية تفعيل الأمر على الجهاز

```
Router(config)#service password-encryption
```


بعد عملية تفعيل الأمر و عملية التشفير

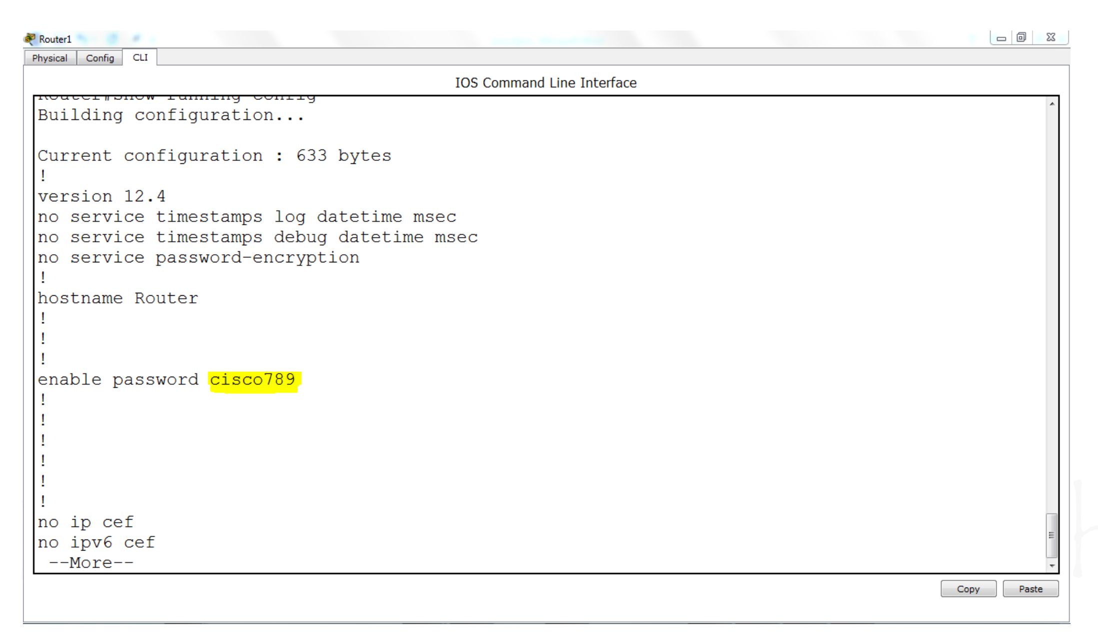
```
Router1
Physical  Config  CLI
IOS Command Line Interface
ip flow-export version 9
!
!
!
!
!
!
!
line con 0
 password 7 0822455D0A16544541
 login
!
line aux 0
 password 7 08751918
 login
!
line vty 0 4
 login
!
!
!
end
 --More--
Copy  Paste
```

هذا الأمر لعرض ملف الإعدادات Router # **show running-config**

- و يجب تشغيل هذا الأمر ايضاً مهم جداً جداً جداً استخدام هذا الأمر و هذه الطريقة في مستوى الـ **Enable** .
- ملاحظة مهم جداً جداً يجب أن لا نقوم بعمل الخطوة الأولى بوضع كلمة مرور على مستوى الإعدادات لإنه لا يقوم بتشفير كلمة المرور ولكن في هذه الطريقة يقوم بتشفير كلمة المرور بشكلة قوي .

Router (config) # **enable secret cisco789**

هذه الصورة ما قبل عملية التشفير



تشغيل أمر التشفير

```
Router(config)#enable secret cisco789
```

ما بعد عملية التشفير

```
Router1
Physical  Config  CLI
IOS Command Line Interface
!
version 12.4
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname Router
!
!
!
enable secret 5 $1$mERr$B7IJJrJxq2fFyOs8ZEeVD1
!
!
!
!
!
!
no ip cef
no ipv6 cef
!
!
!
 --More--
Copy  Paste
```

- بعد الإنتهاء من وضع كلمات المرور و تأمين الجهاز يجب أن تعلم أن كل هذه الإعدادات لم يتم حفظها و سيتم فقدإنها بمجرد انقطاع التيار الكهربائي عن الجهاز يجب علينا أن نقوم بحفظ هذه الإعدادات بطريقة التالي نقوم بكتابة الأمر التالي لحفظ جميع الإعدادات التي تم عملها على الجهاز :

Router # **copy running-config startup-config**

- هذا الأمر من أهم الاوامر التي يجب كتابته في نهاية العمل على الجهاز ليتم حفظ كل شيء تم عملها من إعدادات .

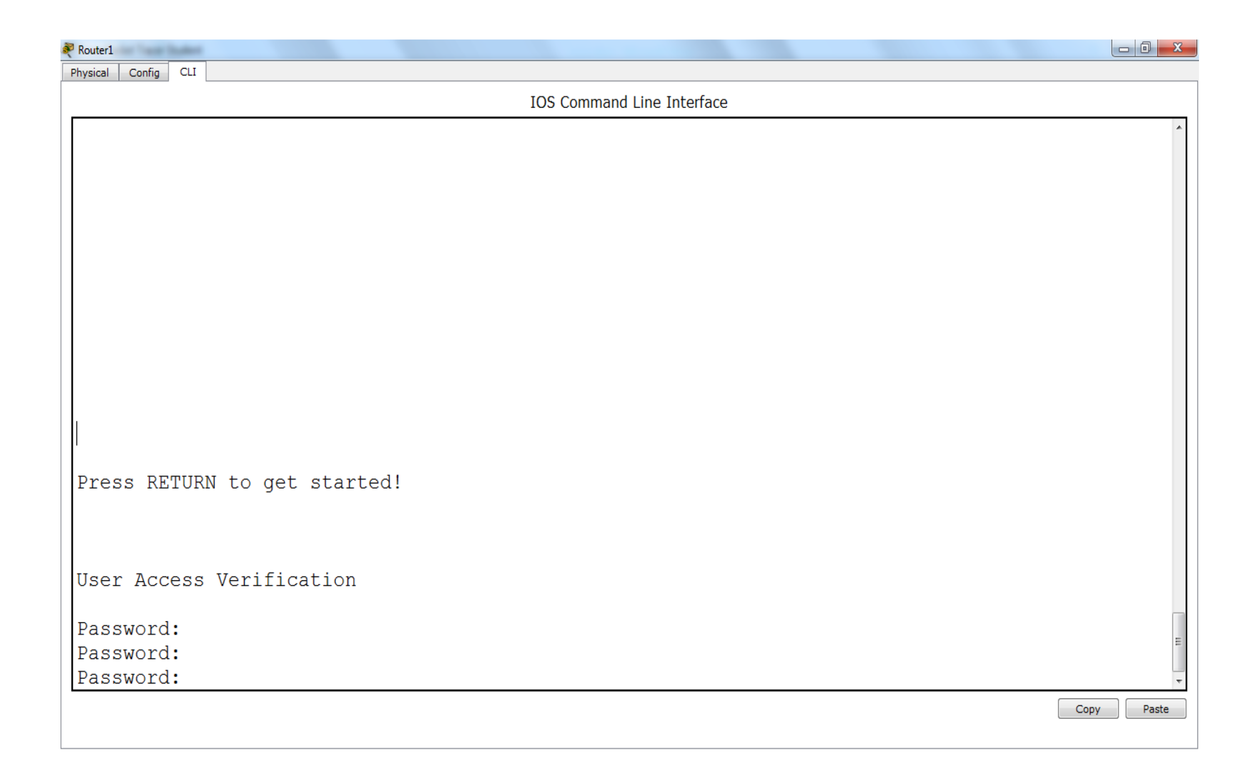
```
Router#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
```

في هذه الصورة بعد كتابة الأمر نقوم بضغط على **Enter** ستظهر رسالة تقول لك هل تريد حفظ الملف بنفس الاسم إذا انتا موفق اضغط **Enter** , و انصحك أن لا تغير أو تعدل في أسم الملف اترك الملف كما هو مسمى .

طريقة أسترجاع كلمة المرور

Password Recovery

في هذا الدرس سأقوم بشرح طريقة أسترجاع كلمة المرور في حال تم ضياعها أو فقدإنها .

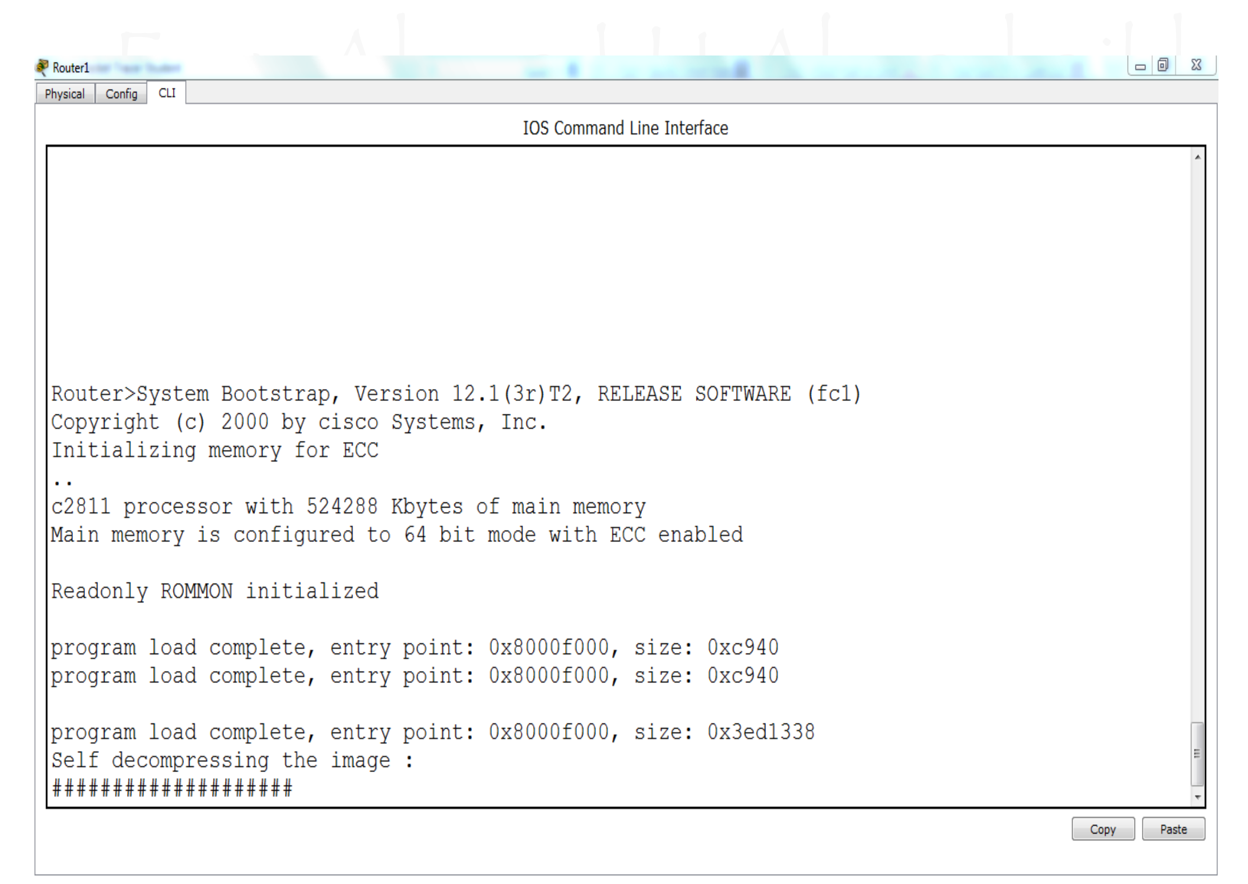


الخطوات :

١- يجب أن يكون جهاز الراوتر متصل بكابل الـ **Console** بشكل مباشر .
٢- يجب إطفاء جهاز الراوتر من مقبس الكهرباء الموجود في خلف جهاز الراوتر و اعادة تشغيلها مرة اخرى بشكل طبيعي و بمجرد إنه يقوم بتحميل النظام قم بضغط على **Ctrl + C** لتقوم بي ايقاف عملية تحميل نظام التشغيل .
٣- بعد عملية الايقاف سيتم تحويلك على مستوى خاص يسمى **Rommon**.
٤- سنقوم بعملية تغير ارقام الريجستري ليتم الدخول على نظام تشغيل اخرى سنقوم بكتابة الأمر هذا **Rommon > confreg 0x2142** قم بضغط على **Enter** و بعده اكتب **Rommon > reset** لتتم عملية اعادة تشغيل الجهاز و الدخول على النظام الآخر .

ملاحظة مهم جداً جداً : عندما نقوم بهذه الخطوات سيتم الإنتقال من قيمة الريجستري الاصلية إلى قيمة ريجستري ثاني .

- **الأن ناتي للتطبيق العملي :** الصورة الظهرة اسفل هذه بعد عملية اطفاء جهاز الراوتر و اعادة تشغيله نرى إنه يقوم بعملية تحميل لنظام التشغيل في هذه الحاله اضغط **Ctrl + C** لي ايقاف هذه العملية و التحويل لمستوى الـ **Rommon** .



أنظر بعد الضغط على Ctrl + C تم التحويل لمستوى الـ Rommon .

```
Router1
Physical | Config | CLI
IOS Command Line Interface

System Bootstrap, Version 12.1(3r)T2, RELEASE SOFTWARE (fc1)
Copyright (c) 2000 by cisco Systems, Inc.
Initializing memory for ECC
..
c2811 processor with 524288 Kbytes of main memory
Main memory is configured to 64 bit mode with ECC enabled

Readonly ROMMON initialized

program load complete, entry point: 0x8000f000, size: 0xc940
program load complete, entry point: 0x8000f000, size: 0xc940

program load complete, entry point: 0x8000f000, size: 0x3ed1338
Self decompressing the image :
########
monitor: command "boot" aborted due to user interrupt
rommon 1 >
rommon 1 >
rommon 1 >
rommon 1 >
rommon 1 >
rommon 1 >
Copy  Paste
```

الأن سنقوم بكتابة الأمر التالي : Rommon > **confreg 0x2142**

و بعد تنفيذ الأمر الأول نقوم بتنفيذ الأمر هذا ليتم اعادة التشغيل Rommon > **reset**

الأن بعد تنفيذ الاوامر أنظر للصورة الراوتر يقوم بعمل اعادة تشغيل.

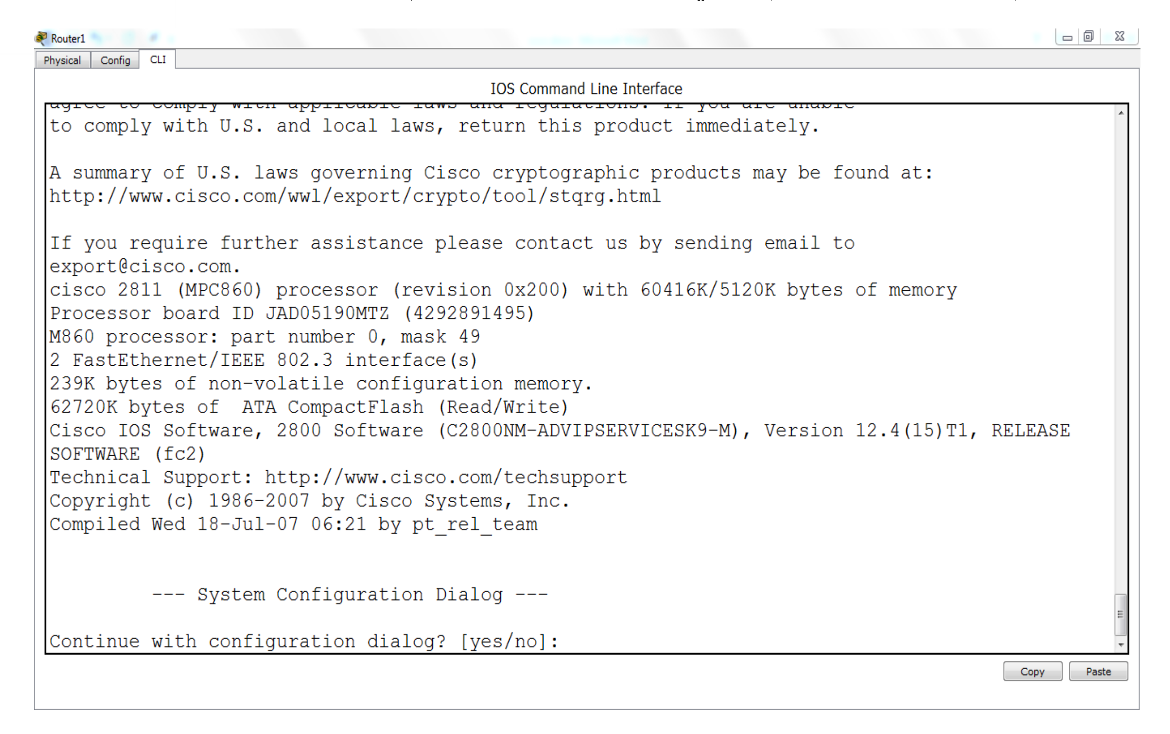
```
Router1
Physical | Config | CLI
IOS Command Line Interface
monitor: command "boot" aborted due to user interrupt
rommon 1 >
rommon 1 >
rommon 1 >
rommon 1 >
rommon 1 >
rommon 1 > confreg 0x2142
rommon 2 > reset
System Bootstrap, Version 12.1(3r)T2, RELEASE SOFTWARE (fc1)
Copyright (c) 2000 by cisco Systems, Inc.
Initializing memory for ECC
..
c2811 processor with 524288 Kbytes of main memory
Main memory is configured to 64 bit mode with ECC enabled

Readonly ROMMON initialized

program load complete, entry point: 0x8000f000, size: 0xc940
program load complete, entry point: 0x8000f000, size: 0xc940

program load complete, entry point: 0x8000f000, size: 0x3ed1338
Self decompressing the image :
#########################
Copy  Paste
```

الأن تم الدخول على النظام الثاني أنظر للصورة اسفل تم الدخول من دون كلمة مرور .



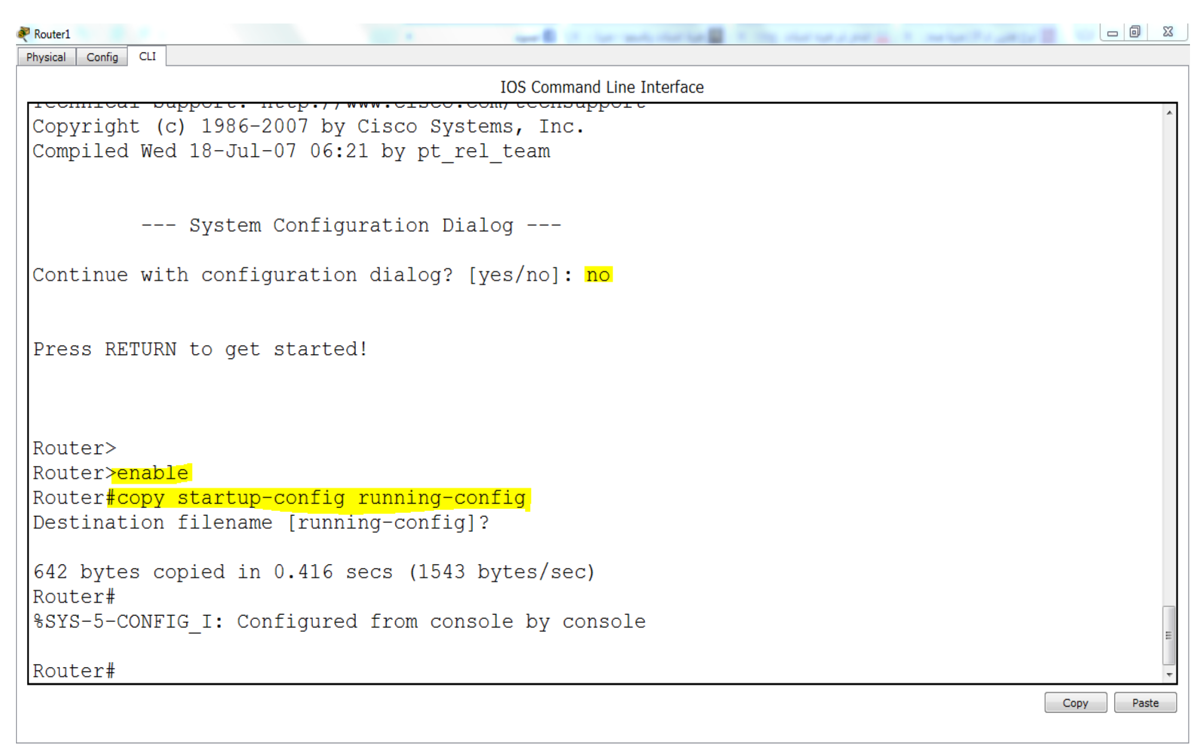
سنقوم بكتابة No و الدخول للتالي :

الأن سنقوم بكتابة الاوامر التالية :

Router > **enable**

Router # **copy startup-config running-config**

كما هو موجود في الصورة التالية :



الأن بعد تنفيذ هذه الاوامر و بعد الضغط على **Enter** سنقوم باستكمال الخطوات الباقية .

الأن سنقوم بكتابة الاوامر التالية :

Router # **show running-config**

هذا الأمر يستخدم لعرض ملف الإعدادات

Router (config) # **no enable secret**

هذا الأمر لي الغاء كلمة المرور الخاص في مستوى الإعدادات

Router (config) # **line console 0**

Router (config-line) # **no password**

هذا الأمر لي الغاء كلمة المرور الخاصة في منفذ الإعدادات Console

Router (config-line) # **exit**

للخروج من المستوى الفرعي

Router (config) # **line aux 0**

Router (config-line) # **no password**

هذا الأمر لي الغاء كلمة المرور الخاصة في منفذ التحكم عن بعد Aux

Router (config-line) # **exit**

للخروج من المستوى الفرعي

Router (config) # **no service password-encryption**

هذا الأمر لي الغاء خدمة تشفير كلمة المرور

Router (config) # **config-register 0x2102**

هذا الأمر مهم جداً جداً و هو أرجاع قيمة الريجستري للقيمة الاصلية للنظام

Router (config) # **end**

للخروج إلى آخر مستوى

Router # **Copy running-config startup-config**

هذا الأمر الذي يقوم بحفظ ملف الإعدادات التي تم العمل عليه أو التعديل عليها

- في هذه الصورة تم تنفيذ امر **Show running-config**

لعرض محتويات الملف تم عرض ملف الإعدادات لاحظ إنه يوجد كلمة مرور.

Router1
Physical Config CLI

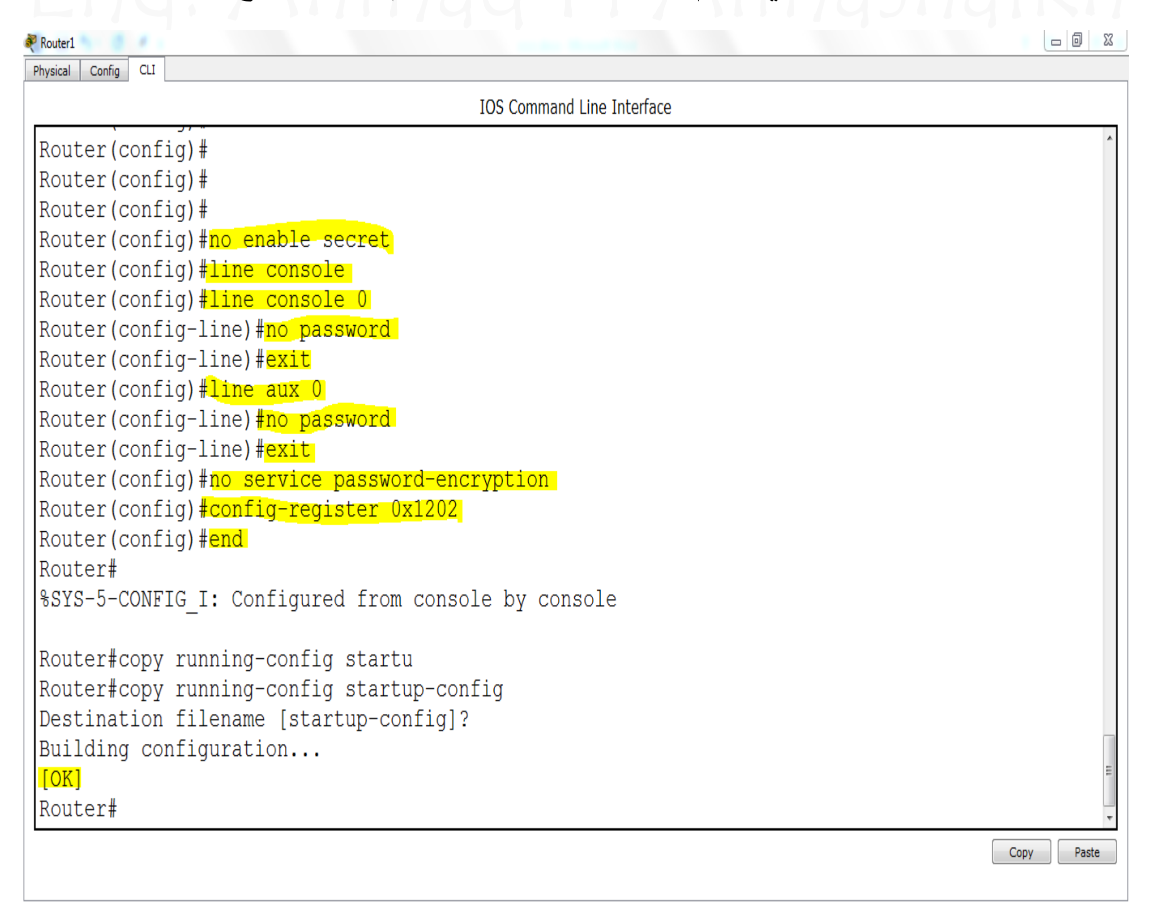
IOS Command Line Interface

```
Router#show running-config
Building configuration...

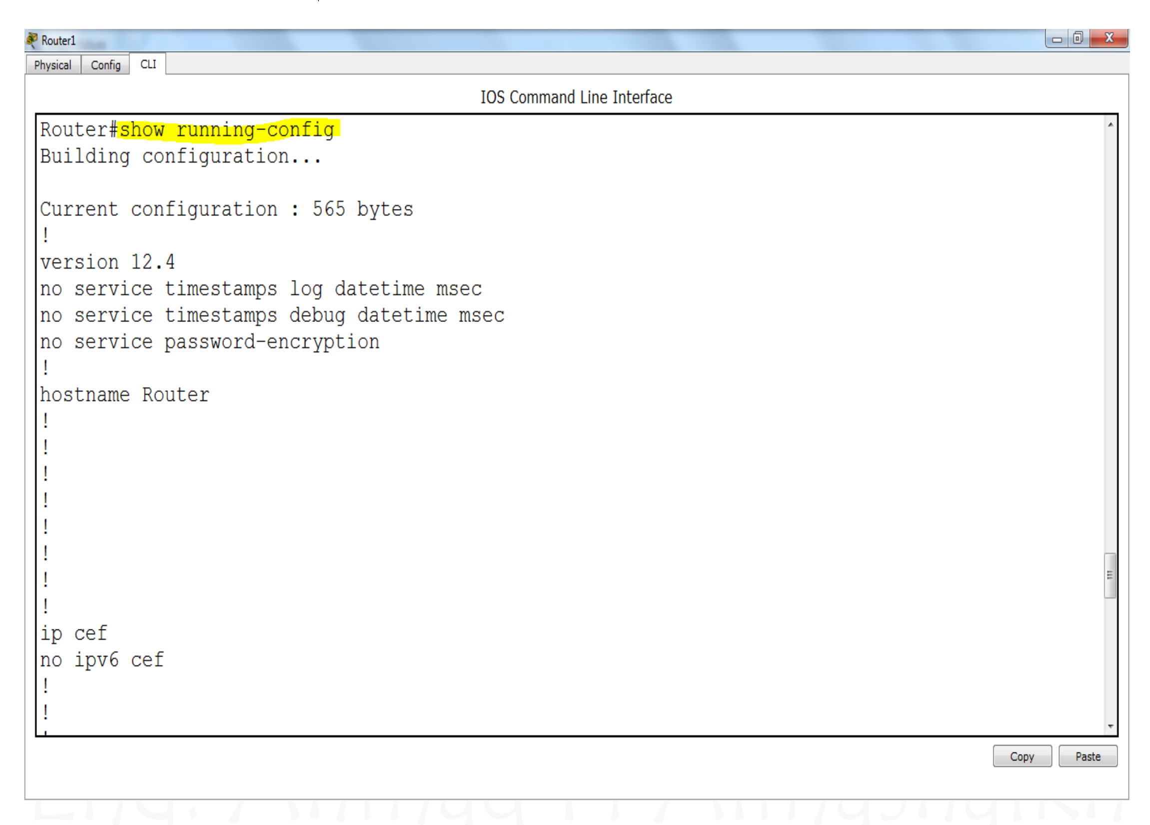
Current configuration : 642 bytes
!
version 12.4
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Router
!
!
!
enable secret 5 $1$mERr$gyuIXJhnplcKI.3q1Kd2a/
!
!
!
!
!
!
ip cef
no ipv6 cef
```

Copy Paste

- في هذه الصورة تم تنفيذ جميع الاوامر التي تم ذكره مسبقاً و لاحظ في نهاية الصورة تم اعطاء **OK** بمعنى إنه تم تنفيذ كل الاوامر بنجاح و تم تعديل رقم الريجستري و الرجوع للقيمة الاصلية الخاص في نظام التشغيل بهذه الطريقة تم حذف جميع كلمات المرور .



- الأن قم بتنفيذ امر **Show running-config** لعرض ملف الإعدادات و نتاكد هل تم ازالة كلمات المرور أو لا لاحظ إنه لا وجود لي اية كلمات مرور تم حذفهم جميعاً.
- أنظر هنا لا يوجد كلمة مرور على مستوى الـ **Enable** لقد تم حذفها .



- أنظر هنا لا يوجد كلمة مرور على المنافذ لا على منفذ الإعدادات و لا على منفذ التحكم عن بعد **Aux Port** , **Console Port** .

Router1
Physical Config CLI
IOS Command Line Interface

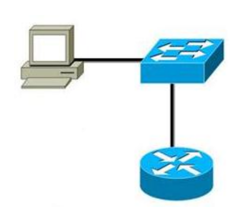
```
!
ip flow-export version 9
!
!
!
!
!
!
!
line con 0
 login
!
line aux 0
 login
!
line vty 0 4
 login
!
!
!
end

 --More--
```

Copy Paste

الوصول عن بعد

Remote Access , Telnet



بروتوكول الـ Telnet : هو بروتوكول وتطبيق يستخدم لتسجيل الدخول إلى حاسوب يستعمل عن بعد بروتوكول **TCP/IP** ويسمح للتطبيق و للمستخدم بإصدار أوامر على الحاسوب البعيد كما لو أن المستخدم مسجل دخوله محليا، ويستعمل التطبيق في الغالب واجهة تداخل نصية لا رسومية هنالك بعض مواقع الإنترنت التي توفر برامج تلنت مجانية.

- يعتبر الـ (**Telnet**) بروتوكول من بروتوكولات ال **TCP/IP** للاتصال بأجهزة الكمبيوتر البعيدة، كما أنه تطبيق من تطبيقات **TCP/IP** يتم استخدامه في تشغيل برامج ال (**Telnet**) لكي يتيح إمكانية التحكم عن بعد ويسمح للمستخدم الدخول من حاسوبه الشخصي إلى حاسب آخر وأن يقوم بالعمل كما لو كان متصل مباشرة مع الجهاز البعيد واستخدام مصادره وهذه المصادر ممكن أن تكون **Online** **Services** (**chat** ,**Database**) .

- خدمة ال **Telnet Server** والـ **Telnet Clients** تعملان معاً لكي تسمح للأجهزة البعيدة المركبة على الشبكة باتصال مع بعضها البعض.

- يمكن لمستخدمي خدمة الـ **Telnet Clients** أن يتصلوا من خلالها مع الحواسب البعيدة التي تشغل الـ ,**Telnet Server** ومن ثم تشغيل التطبيقات على الأجهزة الموجودة على الشبكة أو إنجاز مهام إدارية عليها.إن نوع الجلسة الذي يتم إنشاءه يعتمد على الكيفية التي تعمل بها برامج الـتي تستخدم الـ **Telnet** .
مثل الألعاب وإدارة الأنظمة، وعملية محاكاة الـ **Local Logon** هي مثال نموذجي على استخدام الـ **Telnet** .

- **كيف يتم الاتصال :** يتم الاتصال باستخدام تطبيق الـ (**Telnet**) الموجود على الجهاز المتصل حيث يقوم بالاتصال بتطبيق (**Telnet**) الموجود على الجهاز البعيد (الهدف) وفق مايلي: أولا يبدأ الاتصال من جهاز الكمبيوتر المحلي المتصل إلى البرتوكول الموجود أيضاً على جهاز الكمبيوتر المحلي المتصل ثم ينتقل على شبكة الاتصال إلى البرتوكول (**Telnet**) الموجود على الجهاز البعيد ثم إلى خدمة ال (**Telnet**) الموجودة على الجهاز.

- **مميزات خدمة الـ Telnet :**

١. يمكنك استخدام الـ **Telnet** كمتصفح ويب لأي موقع، ولكنه سيعرض لك مصدر الصفحة حصرا أي الـ **Source** للصفحة، وذلك لأن خدمة الـ **Telnet** كانت تُستخدم عندما ا كانت مواقع الإنترنت مجرد نصوص.

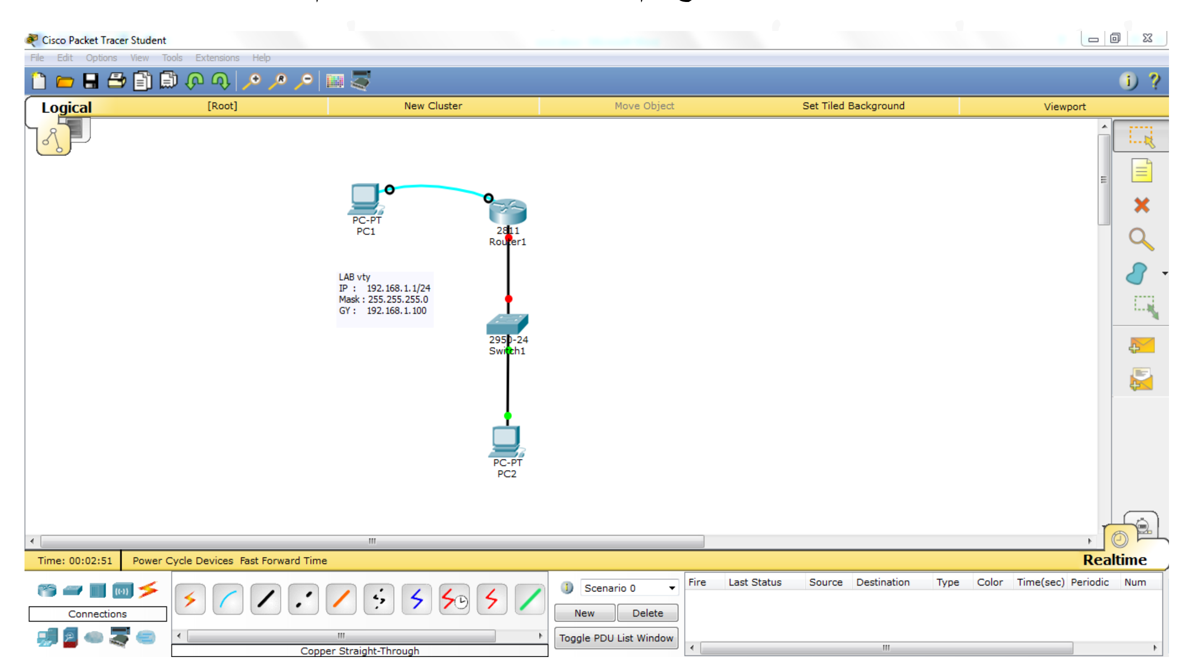
٢. ويمكن استخدام ال **Telnet** أيضا كـ **FTP Client** وذلك باستخدام أوامر يتم إدخالها من خلال الـ **Telnet**.

٣. ويمكنك من خلال الـ **Telnet** أيضا تصفح الايميل **POP Mail** وقراءة رسائلك الواردة وإرسال ما تريد من رسائل، و هذا طبعا إذا كان الايميل من نوع **POP Mail** و هو اختصار لـ **Post Office Protocol** .

- تعمل خدمة الـ **Telnet** على بروتوكول **TCP** و على **Port 23**.

• الأن سنقوم بعمل تطبيق لخدمة الاتصال عن بعد **Telnet** سنقوم بتطبيق على برنامج الـ **Cisco Packet Tracer Student** و العمل عليه .

هذه صورة من داخل البرنامج تم بناء LAB صغير سأقوم بتطبيق عليه



- لاحظ أن الكابل الذي يربط ما بين الراوتر و السويتش لونه أحمر من الطبيعي جداً أن يكون هكذا لإنه لم يتم تشغيل الإنترفيس الخاص في الراوتر ولم نقم بتركيب الاي بي عليه سنقوم في هذه الحال بتشغيل هذا الإنترفيس و تركيب الاي بي عليه و بعده سنقوم بتفعيل خدمة الاتصال عن بعد **vty** و سنقوم بدخول من خلال الجهاز المرتبط في السويتش الذي يرمز عليه **PC 2** و هو من سيقوم بدخول على الراوتر من خلال خدمة الـ **vty** .

- الإعدادات التي سيتم بناء الشبكة عليها .

١- IP : 19.168.1.1

٢- Mask : 255.255.255.0

٣- GY : 192.168.1.100

٤- Interface FastEthernet 0/0

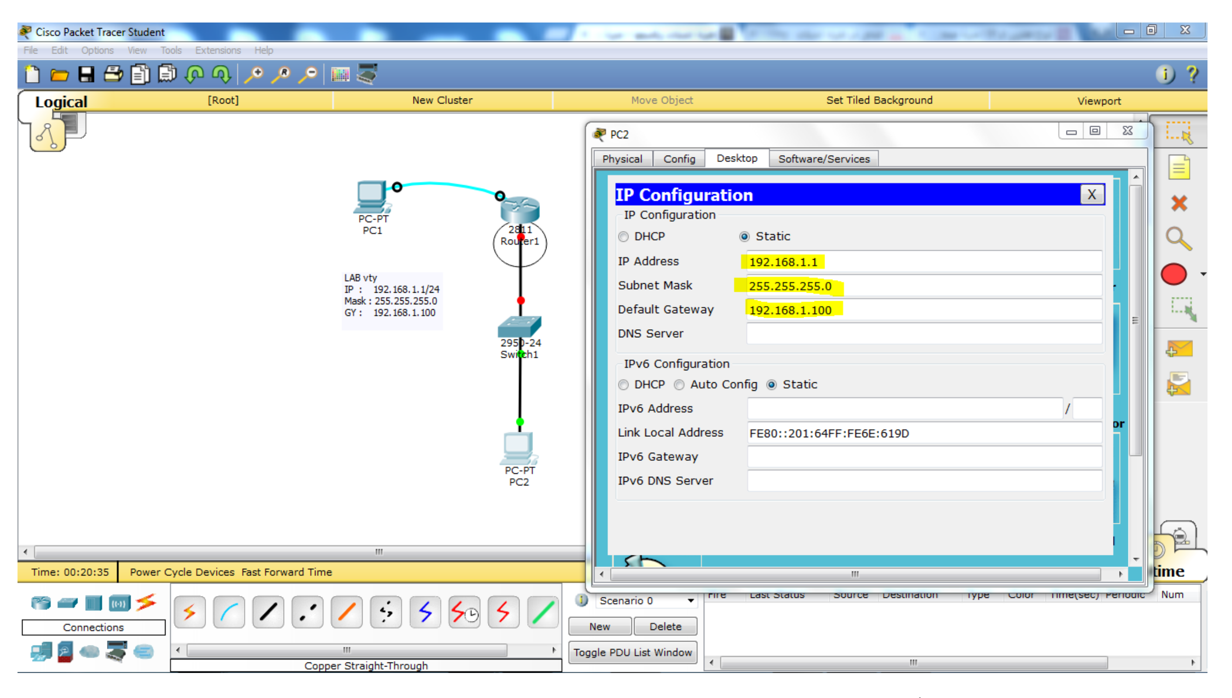
الإنترفيس الخاص في الراوتر المتصل في السويتش .

- الأن سنقوم بوضع الإعدادات و تركيب الاي بي على كل من جهاز الراوتر و جهاز الحاسوب , تابع الطريقة التالية .

PC 2

١- IP :192.168.1.1
٢- Mask : 255.255.255.0
٣- GY : 192.168.1.100

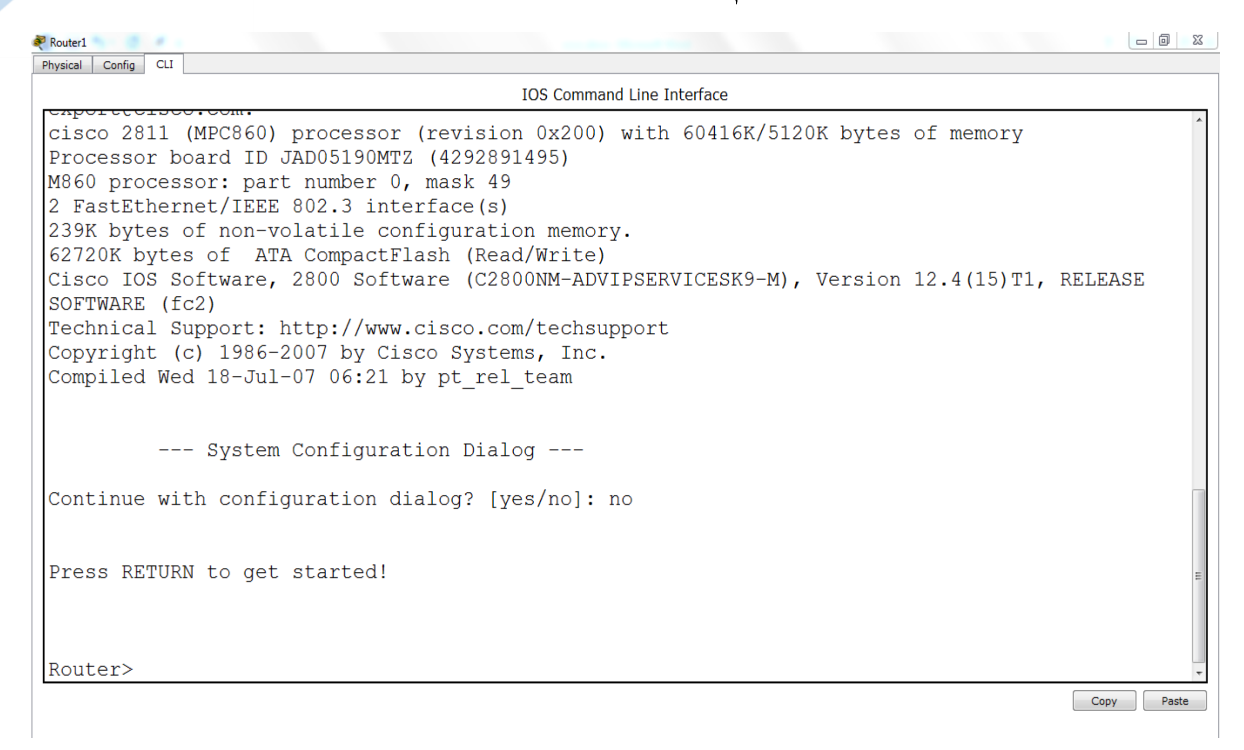
كما في الصورة التالية



- بهذه الطريقة لقد قمناً بتركيب الاي بي على جهاز الحاسوب الأن سنقوم بعمل الإعدادات الخاصة في جهاز الراوتر سنقوم بتشغيل الإنترفيس **0/0** و نقوم بوضع الاي بي عليه و من بعد ذالك نقوم بتفعيل خدمة الـ **vty** تابع التالي .

- الأن سنقوم بدخول على جهاز الراوتر كما سبق لنا أن قمنا بدخول من قبل على جهاز الراوتر مثل ما يتواجد في الصورة التالية :

سنقوم بكتابة No و الاستكمال


Router1
Physical Config CLI
IOS Command Line Interface

```
cisco 2811 (MPC860) processor (revision 0x200) with 60416K/5120K bytes of memory
Processor board ID JAD05190MTZ (4292891495)
M860 processor: part number 0, mask 49
2 FastEthernet/IEEE 802.3 interface(s)
239K bytes of non-volatile configuration memory.
62720K bytes of  ATA CompactFlash (Read/Write)
Cisco IOS Software, 2800 Software (C2800NM-ADVIPSERVICESK9-M), Version 12.4(15)T1, RELEASE
SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2007 by Cisco Systems, Inc.
Compiled Wed 18-Jul-07 06:21 by pt_rel_team


         --- System Configuration Dialog ---

Continue with configuration dialog? [yes/no]: no


Press RETURN to get started!



Router>
```

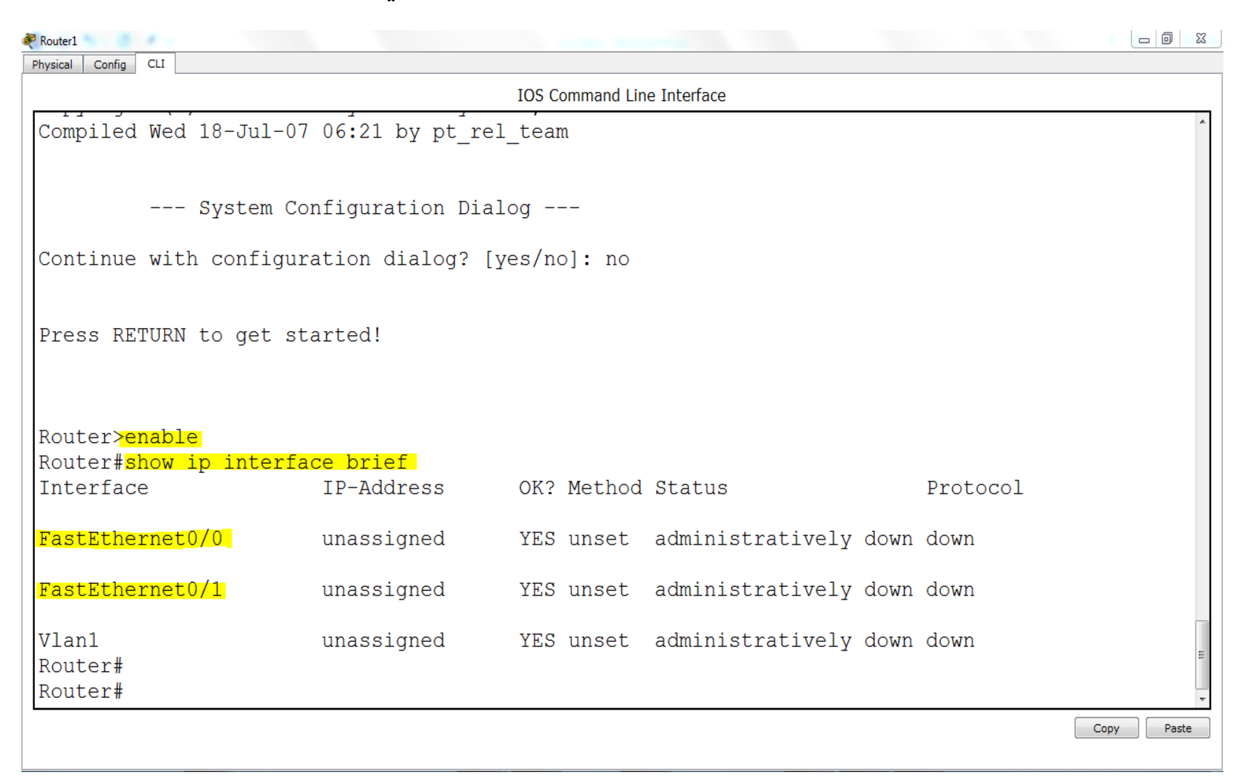
Copy Paste

الأن سنقوم بكتابة الاوامر التالية :

Router > **enable**

Router # **show ip interface brief**

هذا الأمر لعرض الإنترفيس الموجودة على الراوتر كما هو في الصورة التالية


Router1
Physical Config CLI
IOS Command Line Interface

```
Compiled Wed 18-Jul-07 06:21 by pt_rel_team


         --- System Configuration Dialog ---

Continue with configuration dialog? [yes/no]: no


Press RETURN to get started!



Router>enable
Router#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol

FastEthernet0/0        unassigned      YES unset  administratively down down

FastEthernet0/1        unassigned      YES unset  administratively down down

Vlan1                  unassigned      YES unset  administratively down down
Router#
Router#
```

Copy Paste

- الأن يظهر في الصورة السابقة **Interface fast Ethernet 2** الأول ياخذ رقم **0/0** و الثاني ياخذ رقم **0/1** نحن الأن سنقوم باختير الإنترفيس الأول **0/0** سنقوم بتشغيله و تركيب الاي بي عليه .

- **الأن سنقوم بكتاية الاوامر التالية :**

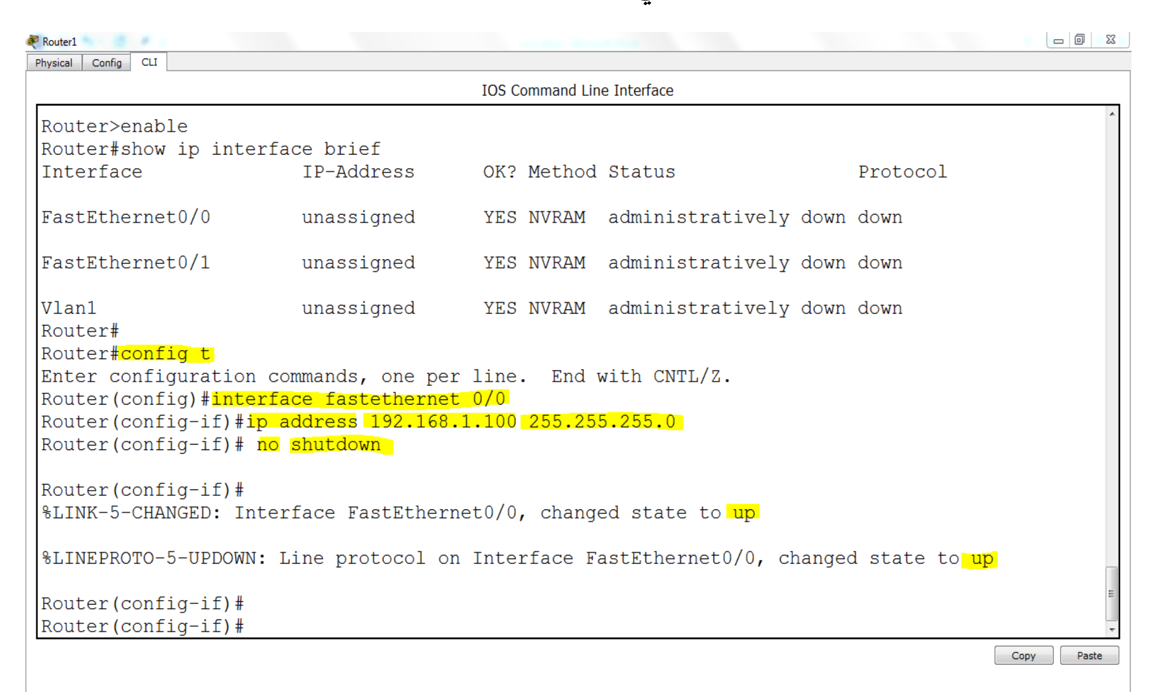
Router # **config t**

Router (config) # **interface fastethernet 0/0**

Router (config-if) # **ip address 192.168.1.100 255.255.255.0**

Router (config-if) # **no shutdown**

كما في الصورة التالية



- لاحظ بعد أن تم تنفيذ الاوامر و تشغيل الإنترفيس **0/0** و تركيب الاي بي عليه تم اظهار رسالة تقول لك أن الإنترفيس تم تشغيله و بحالة **up** و تم تركيب الاي بي عليه الأن نقوم بعملية الخروج من مستوى الإنترفيس و الرجوع إلى المستوى الأول للرجوع نكتب الأمر التالي .

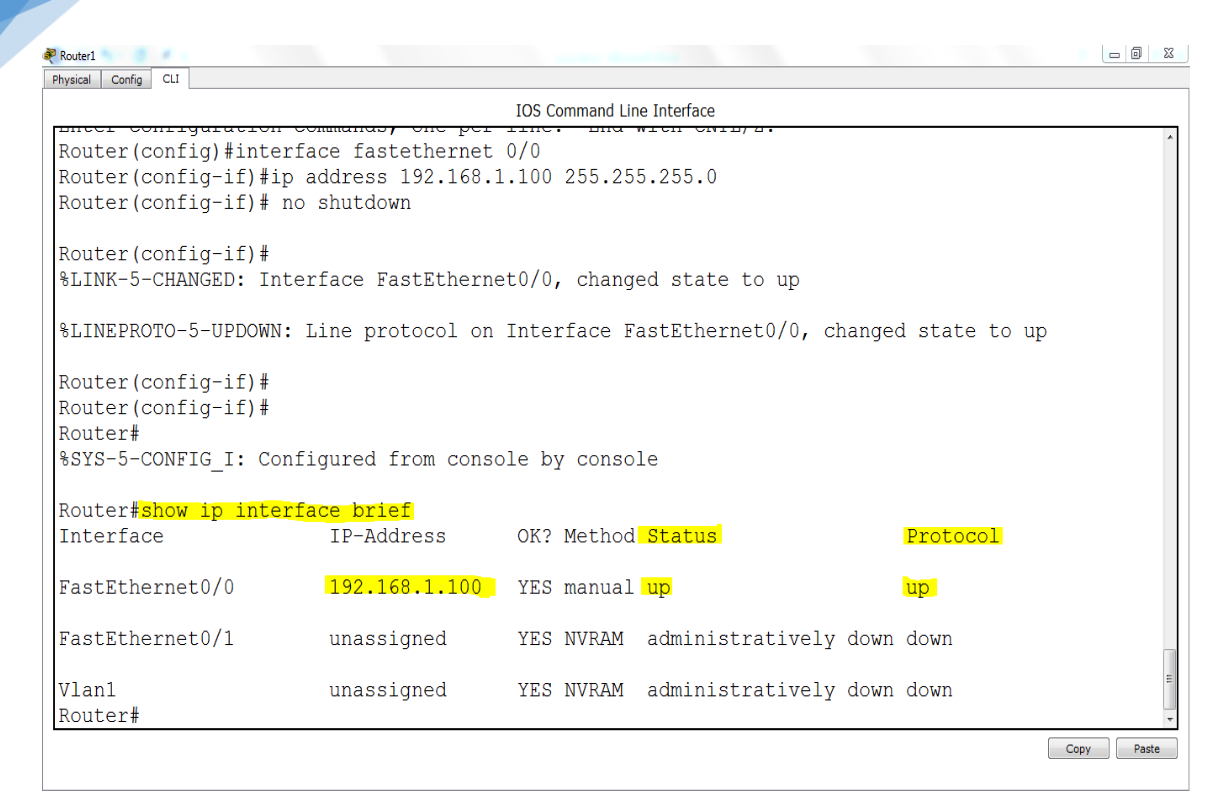
Router (config-if) # **end**

أو نقوم بضغط على **Ctrl + C**

بعد هذا

سنقوم بكتابة الأمر التالي : Router # **show ip interface brief**

و سيظهر لنا الإعدادات التالية التي في الصورة



- لاحظ إنه تم إضافة الاي بي **192.168.1.100** على الإنترفيس **0/0** و الحالة **up** و البروتوكول **up** و لكن لا يوجد لدينا بروتوكول مفعل في الوقت الحالي .

- الأن بعد أن قمنا بعمل الإعدادات و تشغيل الإنترفيس و تركيب الاي بي على الإنترفيس سنقوم الأن بتفعيل بروتوكول الاتصال عند بعد **vty** تابع الدرس .

- طريقة تشغيل أو تفعيل بروتوكول الـ **vty** على أجهزة سيسكو :

- **الأن سنقوم بكتابة الاوامر التالية :**
- هذه إعدادات بروتوكول الـ **vty** .

Router > **enable**

Router # **config t**

Router (config) # **line vty 0**

رقم **0** يعني رقم المنفذ بمعنى انك تستطيع أن تقوم بإضافة اكثر من منفذ من **0** إلى **4**

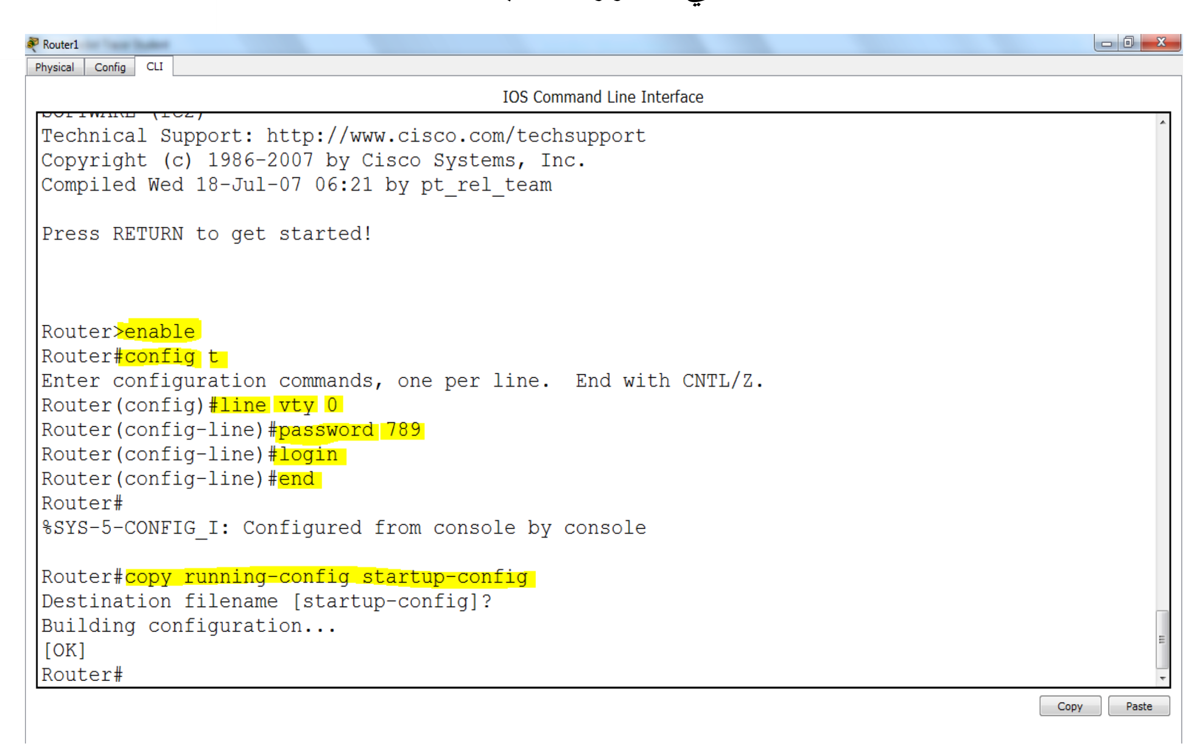
Router (config-line) # **password cisco123**

Router (config-line) # **login**

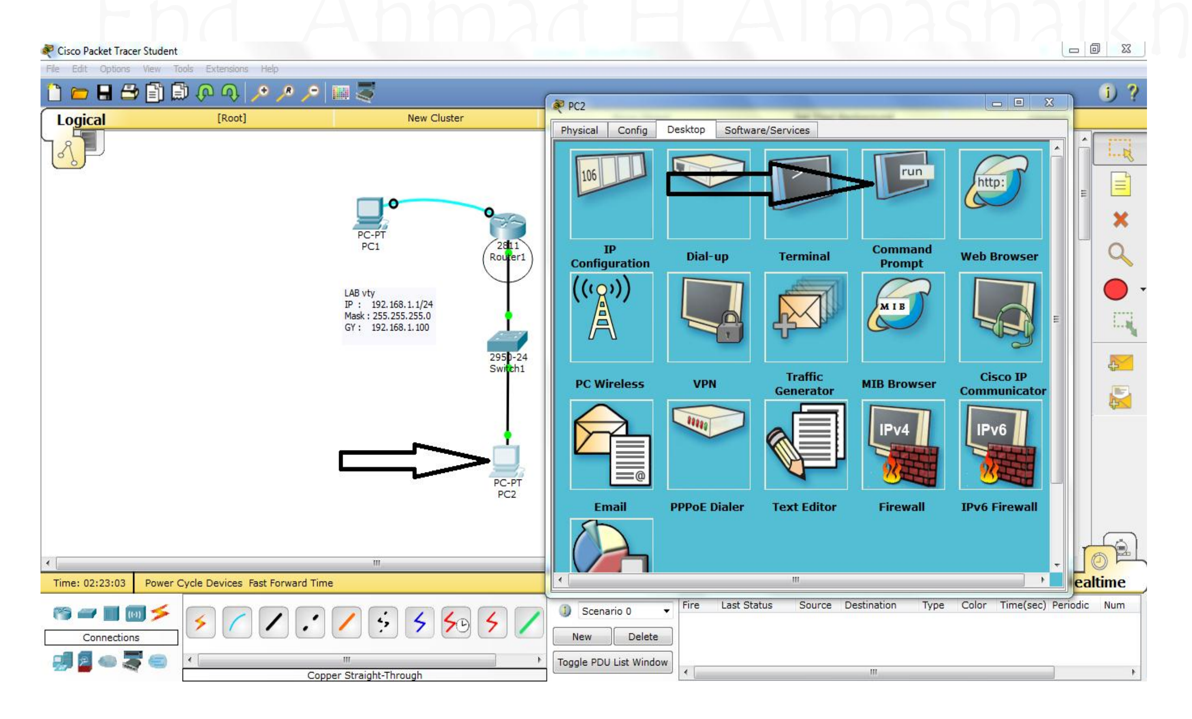
Router (config-line) # **end**

Router # **copy running-config startup-config**

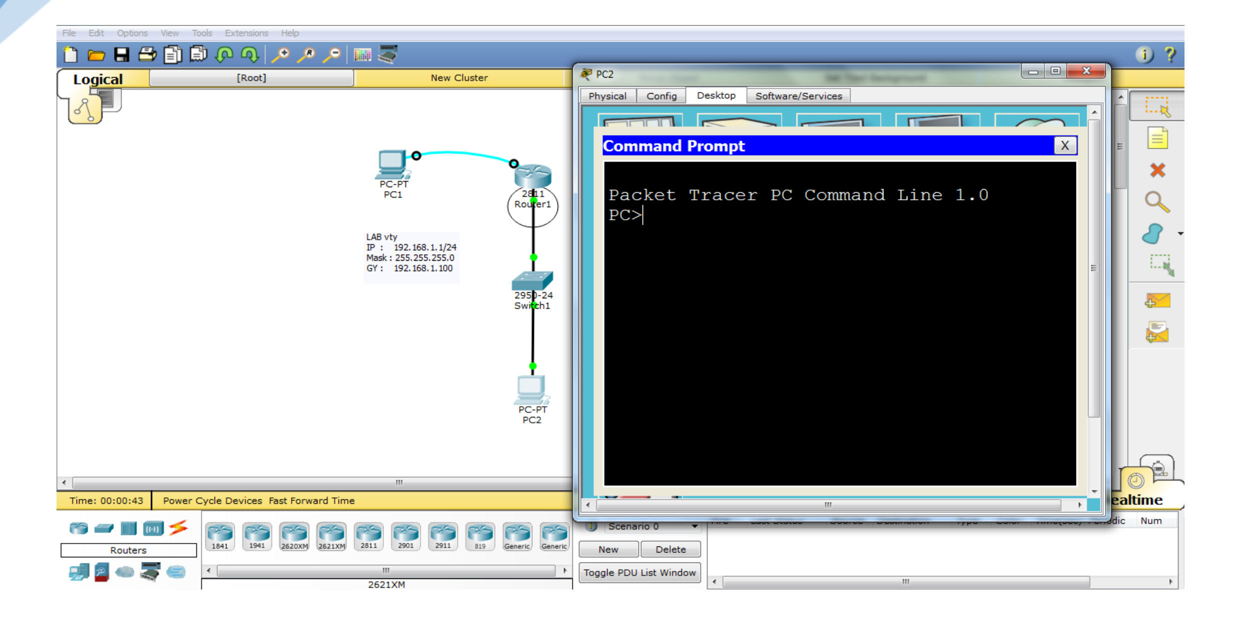
كما في الصورة التالية



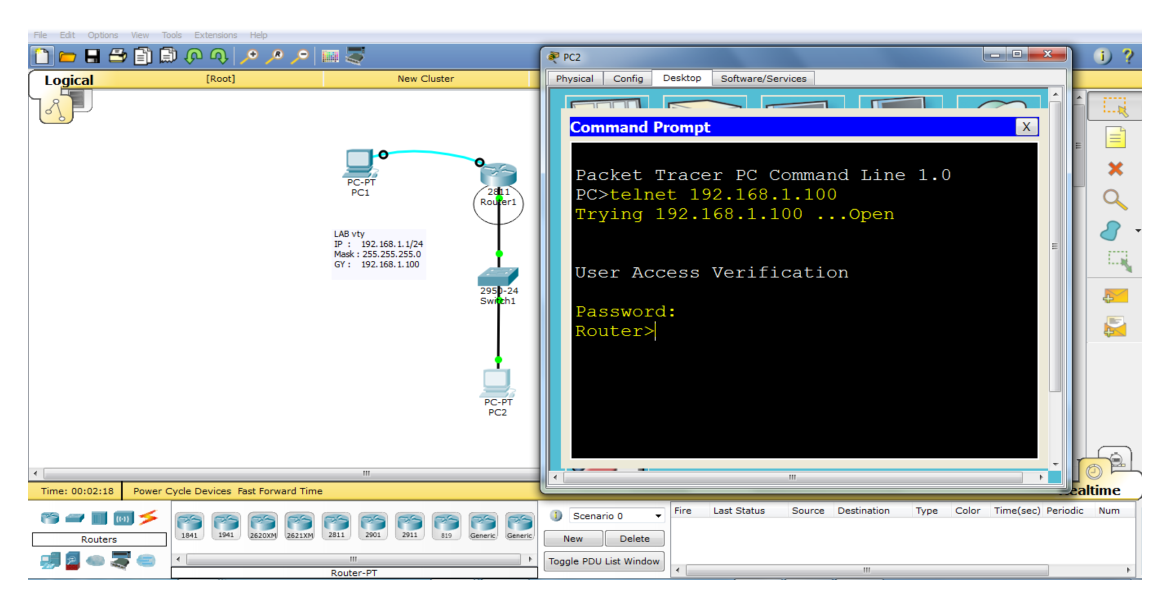
- بعد هذا سنقوم بدخول على الجهاز التالي المسمى **PC 2** و نقوم بدخول على **Command Prompt** كم هو موضح في الصورة التالية :



- و بعد الدخول **Command Prompt** ستظهر شاشة سودا تسمى **DOS** سنقوم بكتابة الاوامر التالية ليتم الدخول و الاتصال في جهاز الراوتر بشكل مباشرة نلاحظ في الصورة التالية .
- في هذه الحالة تم فتح شاشة الدوس سنقوم بكتابة و نقوم بتسجيل الدخول على الراوتر .



- الأن سنقوم بكتابة الاوامر التالية لتسجيل الدخول على الراوتر كما في الصورة التالية :



- **الاوامر التالية لتسجيل الدخول على الراوتر :**

PC > **telnet 192.168.1.100**

هذا الأمر يقوم بعملية الاتصال في الراوتر بعد أن يتم الاتصال سيطلب منك كلمة المرور التي تم وضعها في الإعدادات كلمة المرور هي **789** .

- هذه طريقة إعدادات بروتوكول الـ **vty** ولكن يجب المعرفة أن هذا البروتوكول ينقل البيانات بشكل عادي و غير مشفر بمعنى يمكن سرقة و مراقبة البيانات و انت متصل على جهاز الراوتر و لهذا السبب قاموا بتطوير هذا البروتوكول تم إضافة خاصية الحماية و عليه و هي **SSH** تستخدم لتشفير الاتصال ما بين المستخدم و جهاز الراوتر سنقوم بشرح هذه الخاصية و كيفية إعدادات هذه الخاصية مع بروتوكول **vty** ليتم الاتصال بشكل موثوق و مشفر .

Routing

التوجيه

التوجيه Routing : هو وسيلة مهمة جداً لمستخدمين الشبكات على مختلف أنواع الشبكات طبعاً مثل شبكة الإنترنت والشبكة المحلية و شبكات الشركات و المؤسسات و الكثير من الشبكات الآخر , وظيفة الموجه أن يقوم بتوجيه الـ **Packet** للشبكة المطلوبة بذاتيها و يقوم ايضاً باختير افضل مسار من اصل مجموعة مسارات .

تفصيل أكثر : يقوم الموجه بإرسال الـ **Packet** من شبكة إلى اخرى حتى لو كانت الشبكة تم ربطها بإكثر من موجه في المسار .

- **الوظيفة الرئيسية :** لجهاز الراوتر أو الموجه هي توجيه الـ **Packet** ما بين الشبكات المختلفة وليتم بهذه الوظيفة على أكمل وجه ينبغي أن يكون على معرفة كاملة بمواقع كل الشبكات وإلا سوف يقوم بإهمال الحزم مجهولة الهدف و من وجهة نظر الراوتر أو الموجه فإن موقع أي شبكة يرتبط بأحد المنافذ **Interface** الموجودة عليه لذالك يجب أن تكون هناك طريقة لربط كل الشبكات بالمنافذ الذي يؤدي إليهام و هنا يأتي دور جدول التوجيه **Routing Table** الخاص في الراوتر .

- **جدول التوجيه Routing Table :** جهاز الراوتر يقوم ببناء جدول التوجيه **Routing Table** و يعتمد عليه في تسجيل عناوين الشبكات و مسارات الشبكات و المسافات ما بين الشبكات في كل الفروع و يفيد الجدول في عملية توجيه الـ **Packet** بشكل صحيح.

- **محتويات جدول التوجيه Routing Table :**

١- تحتوي جداول التوجيه للموجهات على عناوين الشبكات المرتبطة معها وليس على عنوان كل جهاز على الشبكة (قد تحوي عناوين بعض الأجهزة) .

٢- يتم تخزين جدول التوجيه في الذاكرة.

٣- يوجد هذا الجدول في كل عقد **IP** على الشبكة التي تحتوي على بروتوكول **TCP/IP** وليس فقط الموجهات.

٤- يتم استخدام هذا الجدول لتحديد عنوان **IP** للعقدة التالية التي سيتم الإرسال لها سواء كان هذا العنوان هو عنوان الحاسب الوجهة(توصيل مباشر) أو عنوان موجه آخر (توصيل غير مباشر) .

٥- يمكن عرض جدول التوجيه بكتابة العبارة (**route print**)على مؤشر الأوامر (**command prompt**) بالإضافة إلي وجود العديد من التعليمات للتعامل معه مثل : **route add , route change ,route delete**.

٦- بعض العناوين ضمن هذا الجدول يتم تعريفها تلقائيا" حتى لو تم حذفها عند الإقلاع.

- **حقول مداخل جدول التوجيه :**

يضم كل مدخل الحقول التالية :

١- **Network ID :** يمثل عنوان الوجهة سواء كانت الوجهة النهائية أو عنوان شبكة أخرى يوجد عليها الوجهة النهائية

٢- **Network mask :** وهو الـ **mask** المقابل لعنوان الـ **IP** الموجود في **network IP**

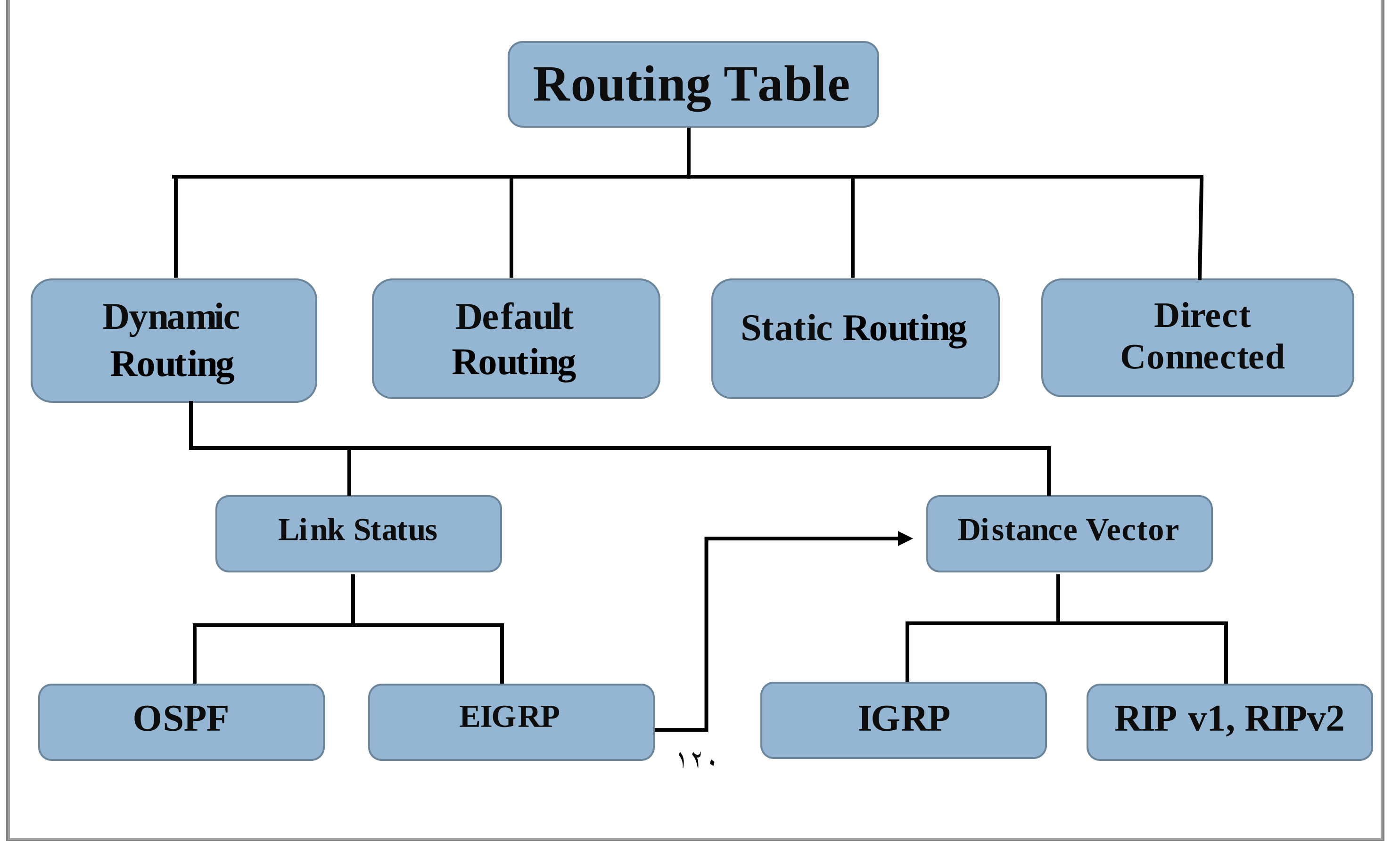
٣- **Gateway :** وهو عنوان العقدة التالية

٤- **Interface :** يتم فيها تحديد **Interface** التي سيتم الإرسال عليها حيث من الممكن أن يكون لحاسب أكثر من كرت شبكة واحد أما إن كنا نتحدث عن موجه فهو حتما" يحوي أكثر من **Interface**

٥- **Metric :** هو رقم يحدد عدد الموجهات ضمن الطريق المسلوك للوصول إلى الوجهة فهو يحدد كلفة الإرسال وبالتالي فهو يستخدم لتحديد الطريق الأفضل

ملاحظة : بحالة **Directly attached network IDs** نضع قيمة **metric** تساوي الواحد أو الصفر على اعتبار أنه لايوجد موجه بين المرسل والمستقبل .

- الغرض من الـ **router** هو اختبار البيانات القادمة إليه لكي يختار أحسن مسار لها ويقوم بتوجيهها معتمدا على **IP address** إضافة إلى أنه يقوم بربط تكنولوجيا الطبقة الثانية **data link layer** المختلفة مثل **Ethernet** و **token-ring** وهذه أحد أهم وظائفه.
- جهاز الراوتر يقوم بعملية الاتصال أو الربط باكثر من طريقة بمعنى إنه يتم بناء جدول التوجيه على أكثر من من شكل كما هو موضح في الجدول التالي :



- سأقوم بشرح كل من هذه الأنواع بشكل مفصل :

١- **Direct Connected:** هذا الاتصال بشكل مباشر بمعنى أن الشبكات المتصلة في الراوتر تم ربطها بشكل مباشرة من غير بروتوكولات ولا إعدادات فقط اتصال مباشر مثل من سويتش إلى الراوتر و, يكون رمزها في جدول التوجيه بحرف " **C** " أختصار لـ **(Connected)** و تكون قيمة المسافة الإدارية **(0)** بمعنى إنه لا يوجد مسافة إدارية و لا عدد قفزات لي إنه اتصال مباشر من و إلى بشكل مباشر.

٢- **Static Routing:** هذا يعني اتصال الشبكات في بعضها البعض عن طريق اوامر يقوم بها مهندس الشبكة بعمل الإعدادات ليتم الاتصال في الشبكات بشكل يدوي من دون أن يقوم بتفعيل بروتوكولات أو ما شابه، في هذه الحالة يتم إنشاء جدول التوجيه بشكل يدوي و عندما نريد إضافة شبكات أو ازالة شبكات نقوم ايضاً بشكل يدوي ,ويكون رمزها في جدول التوجيه بحرف " **S** " أختصار لـ **(Static)** و تكون قيمة المسافة الإدارية **(1)** و عدد القفزات تكون **(0)** أو أكثر على حسب وجود الشبكات و طريقة الاتصال بها.

٣- **Default Routing:** هذا النوع من الاتصال للوصول إلى عنوان شبكة غير موجودة في الشبكة الخاصة بك أو عندما تكون تريد الاتصال بشبكة الإنترنت أو تريد الاتصال بشبكة لا تعرف في اية شبكة موجودة في هذه الحالة يتم إعدادات هذه الاتصال على الراوتر الذي يكون متصل على شبكة الإنترنت ليتم التوصيل في الشبكات الغير معروفة مثل مواقع الإنترنت عندما تريد الاتصال في موقع ولا تعرف عنوان الشبكة الذي عليها هذا الموقع هذا اكبر مثال لهذا الاتصال , قيمة المسافة الإدارية تكون(**1**) و رمزه في جدول التوجيه يكون " **S** " العنوان الذي يعتمد عليه هو **ip : 0.0.0.0 mask : 0.0.0.0** و الـ **Gy : 192.168.1.100** هذه البوابة التي ستقوم بتوصيلك بشبكة الإنترنت .

٤- **Dynamic Routing:** الاتصال بالشبكات الغير متصلة اتصال مباشرة مثل عندما ا تكون لدينا شبكة في منطقة و شبكة اخرى في منطقة اخرى هذه الشبكات لا يوجد بينهم ربط اتصال مباشر ماذا نحتاج لعمل اتصال ما بينهم سنحتاج للبروتوكولات الخاصة في التوجيه ليتم الربط ما بينا الشبكات عن طريق البروتوكولات في الطرفين , يتم تطبيق و إعدادات بروتوكول معين في الشبكة الأولى و سيتم تطبيق و إعدادات نفس هذه الإعدادات في الشبكة الثانية بنفس البروتوكول ليتم التعرف على الشبكات و بناء جدول توجيه بشكل اتوماتيكي ما بين الشبكات من غير تدخل مهندس الشبكة في بناء جدول التوجيه بمعنى إنه سيتم بناء الجدول على معلومات البروتوكول الذي سيتم تشغيلها على الراوتر و كل بروتوكول يكون له قيمة مسافة ادارية خاصة به سنقوم بتعرف عليه و كل بروتوكول يكون له رمز خاص فيه في جدول التوجيه ايضا سنقوم بتعرف عليهم .

- **:Dynamic Routing**

هذا الاتصال يعتمد على بروتوكولات التوجيه الديناميكية **Dynamic Protocols** و يتم تقسيم هذه البروتوكولات على قسيمن قسم يعتمد على السرعة و المسافة و قسم يعتمد على المسافة ولا يعتمد على السرعة في عملية نقل و توجيه الـ **Packet** سأقوم بذكر هذه البروتوكولات مع شرح كل نوع من هذه البروتوكولات .

١- البروتوكولات التي تعتمد على السرعة ولا تهتم للمسافة كما هو موجود في الجدول السابق قمة بذكرها و هي **Link Status Protocol** و يندرج تحت هذا المسمى البروتوكولات التي تهتم في السرعة ولا تهتم في المسافة و من اشهر هذه البروتوكولات برتوكول الـ **OSPF** و **EIGRP** هذه البروتوكولات الضخمة التي تهتم في سرعة النقل و لاتهم للمسافة مهما كانت المسافة .

٢- البروتوكولات التي تعتمد على المسافة ولا تهتم للسرعة كما هو موجود في الجدول السابق قمة بذكرها و هي **Distance Vector** و يندرج تحت هذا المسمى البروتوكولات التي تهتم في المسافة ولا تهتم في السرعة و من اشهر هذه البروتوكولات بروتوكول الـ **IGRP** و **RIP v1** و **RIP v2** هذه البروتوكولات تهتم في المسافة ولا تهتم في السرعة .

٣- **:Dynamic Routing** تعمل ايضاً على نوعاً نوع بوابة داخلية **Interior Gateway Protocols** و نوع بوابة خارجية **Exterior Gateway Protocols** مثل بروتوكولات تعمل في الشبكة الداخلية و بروتوكولات تعمل في الشبكة الخارجية، مثل ما هو موجودة في الجدول التالي اسفل.

	Interior Gateway Protocols				Exterior Gateway Protocols
	Distance Vector Routing Protocols		Link State Routing Protocols		Path Vector
Classful	RIP	IGRP			EGP
Classless	RIPv2	EIGRP	OSPFv2	IS-IS	BGPv4
IPv6	RIPng	EIGRP for IPv6	OSPFv3	IS-IS for IPv6	BGPv4 for IPv6

Classification of Routing Protocols

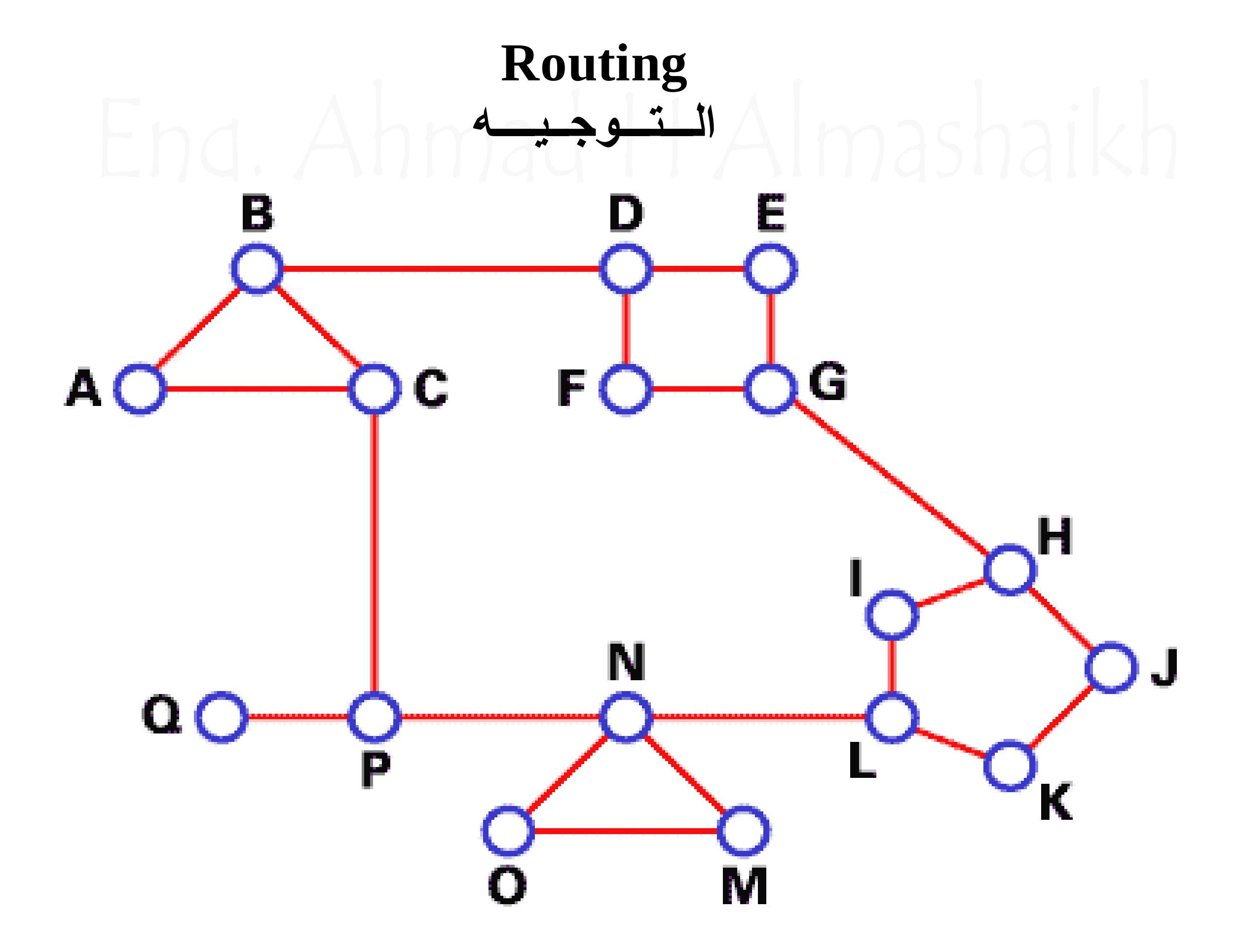
- بنسبه لـ **Classful** و **Classless** سأقوم بشرح كل بروتوكول يدعم هذه الخاصية بتافصيل مع العلم لقد تم شرح هذه الخاصية في الدروس السابقة المستوى الأولى في درس العناوين **IP** , و سأقوم بشرح هذه الخاصية من ناحية البروتوكولات .

- قبل البداء في التطبيق العملي يجب التفريق ما بين الـ **Routing Protocols** و **Routed Protocols** و معرفة الفرق ما بينهم :

- **Routing Protocols:** هو المسؤولة عن تنقل الـ **Packet** ما بين الشبكات، و هي من وظيفة الطبقة الثالثة **Network Layer 3** من طبقات الـ **OSI** و هي الطبقة المسؤولة عن تحديد مسار الـ **Packet** , بمعنى هي البروتوكولات المخصصة لتبادل المعلومات ما بين الراوترات .

- **Routed Protocols:** هي البروتوكولات المهتمة بنقل البيانات **Data** و التاكد من وصولها إلى جميع الراوترات المتصلة في بعضها البعض، بمعنى إنه تقوم بتسجيل أو التعديل في **Routing Table** .

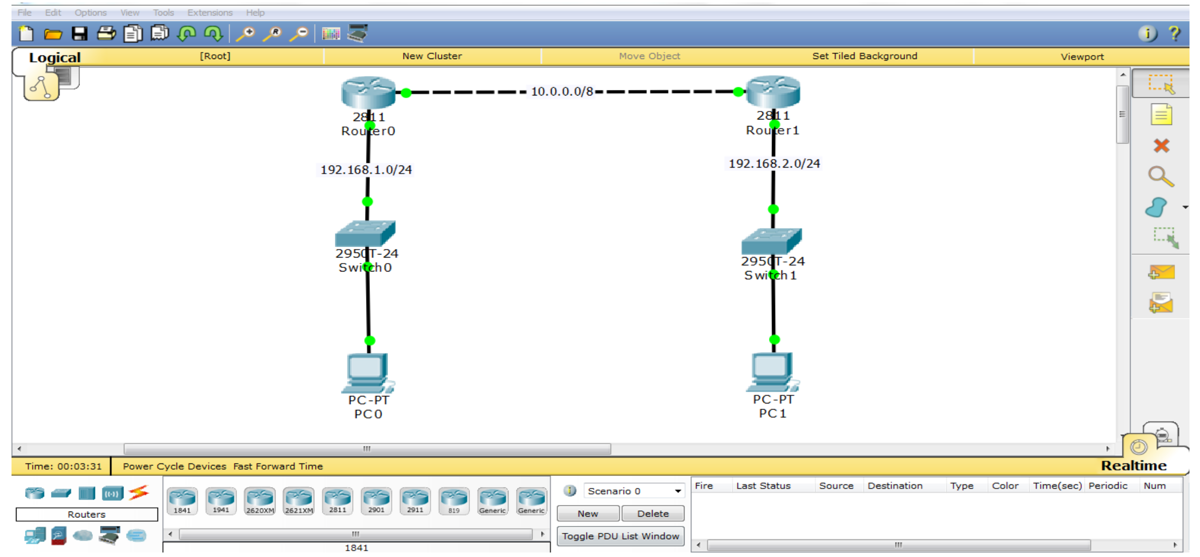
- **ما هي البروتوكولات تعريف بسيط للبروتوكولات :** هي مجموعة من القوانين المتعارف عليه يتم برمجتها على الحواسيب و على أجهزة الراوتر أو الموجهات لكي يتم العمل فيها ما بين الحواسيب أو الراوترات ليتمكنو من الاتصال في بعضهم البعض.



Static Routing IPv4

- سنبداء في التطبيق العملي و سنقوم بعمل إعدادات التوجيه اليدوي **Static Routing**:

- سنقوم ببناء شبكة مكونة من راوترين على برنامج الـ **Cisco Packet Tracer Student** و سنقوم ببرمجة كل راوتر بشكل يدوي و تعريف الشبكات على بعضها البعض كما في الصورة التالية و نجعل كل الشبكات أن تتصل في الشبكات الآخر :



- الإعدادات التي سيتم بناء الشبكة عليها .

- في هذا التصميم يتكون لدينا ثلاث شبكات كل شبكة لها عنوان اي بي .

- الشبكة الأولى **Network (1) :**

IP: 192.168.1.0/24 عنوان الشبكة الأولى.

Mask: 255.255.255.0 عنوان قناع الشبكة.

GY: 192.168.1.100 عنوان بوابة الشبكة و هذا ما سيتم تركيبها على الإنترفيس **f0/0** المتصل من جهاز الراوتر إلى جهاز السويتش.

جهاز الكمبيوتر أو الأجهزة التي في داخل هذه الشبكة سيتم تركيب الاي بي بهذا الشكل:

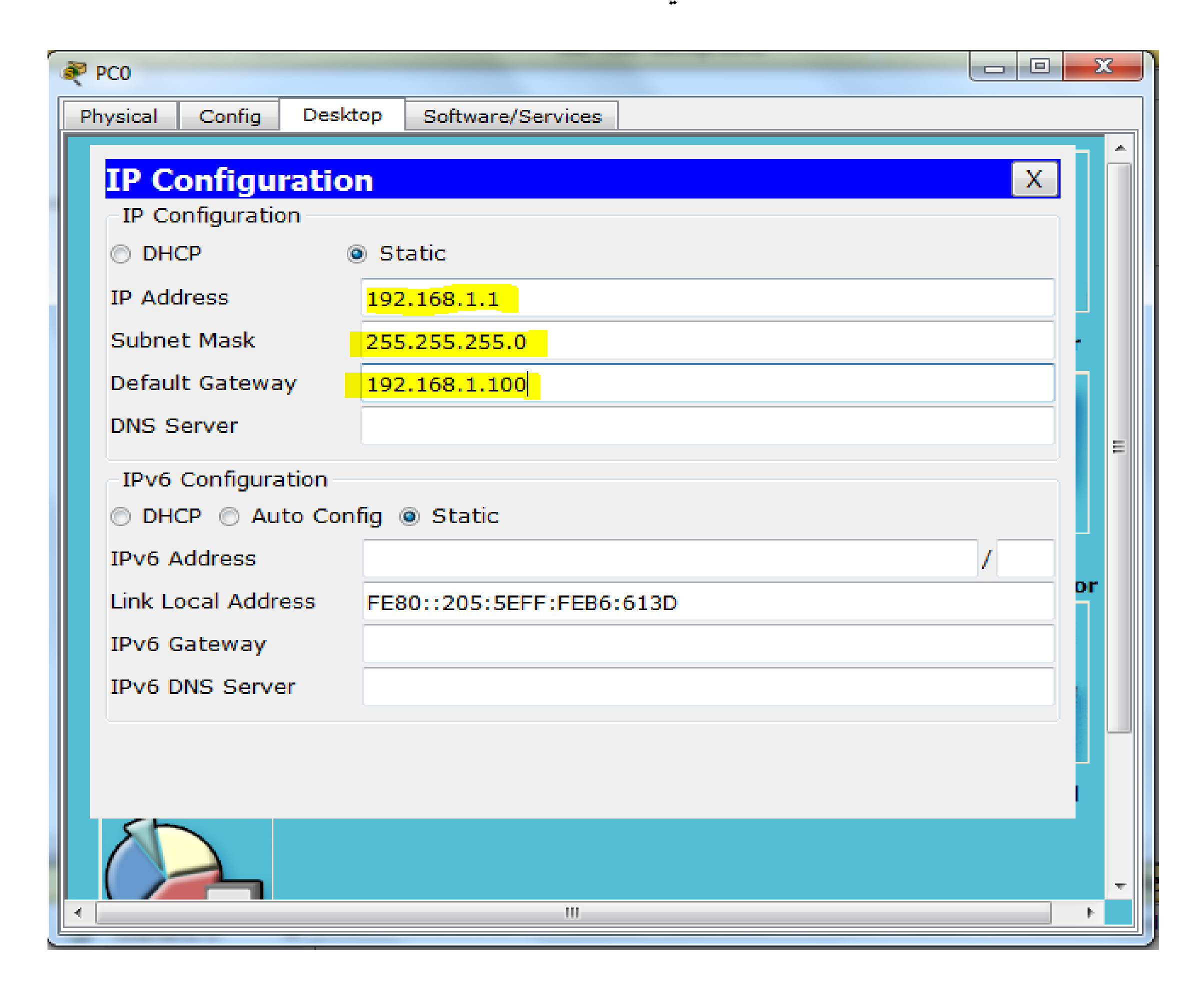
PC 0

IP: 192.168.1.1 عنوان الجهاز.

Mask: 255.255.255.0 عنوان قناع الشبكة.

GY: 192.168.1.100 عنوان بوابة الشبكة في الراوتر.

كما في الصورة التالية



- **الشبكة الثانية (2) Network :**

IP: 192.168.2.0/24 عنوان الشبكة الثانية.

Mask: 255.255.255.0 عنوان قناع الشبكة.

GY: 192.168.2.200 عنوان بوابة الشبكة و هذا ما سيتم تركيبها على الإنترفيس **f0/0** المتصل من جهاز الراوتر إلى جهاز السويتش.

جهاز الكمبيوتر أو الأجهزة التي في داخل هذه الشبكة سيتم تركيب الاي بي بهذا الشكل:

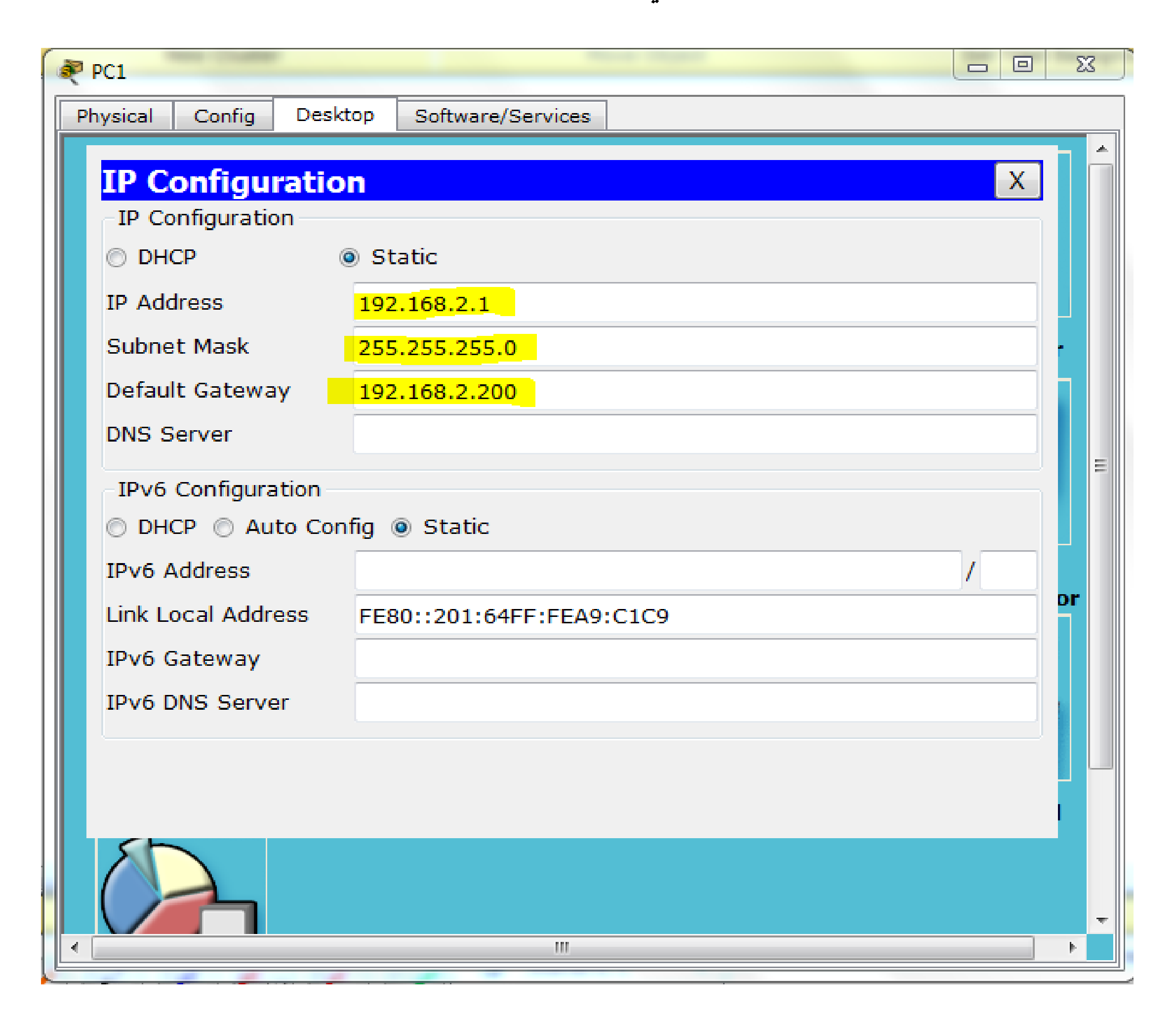
PC 1

IP: 192.168.2.1 عنوان الجهاز.

Mask: 255.255.255.0 عنوان قناع الشبكة.

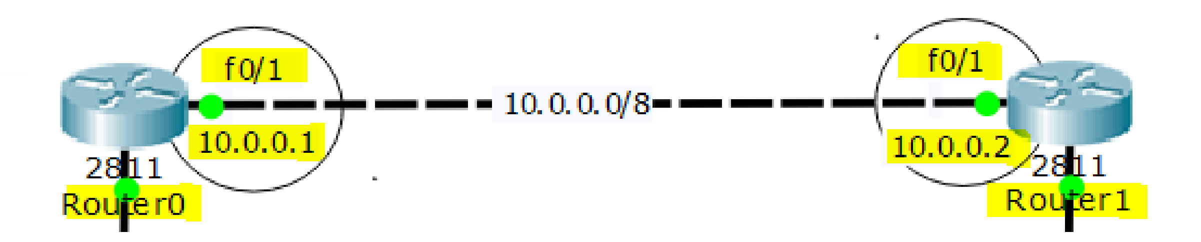
GY: 192.168.2.200 عنوان بوابة الشبكة في الراوتر.

كما في الصورة التالية



- الشبكة الثالثة **Network (3) :**

- هذه الشبكة التي سترتبط ما بين الشبكة الأولى و الشبكة الثانية ليتم الربط و التوصيل ما بين الشبكات سيتم تفعيل هذه الشبكة على الشكل التالي سنقوم بدخول على الراوتر المسمى **Router 0** و نقوم بتشغيل الإنترفيس **f0/1** المتصل في الراوتر المسمى **Router 1** و بعده سنقوم بدخول على الراوتر المسمى **Router 1** و نقوم بتشغيل الإنترفيس **f0/1** المتصل في الراوتر المسمى **Router 0** .



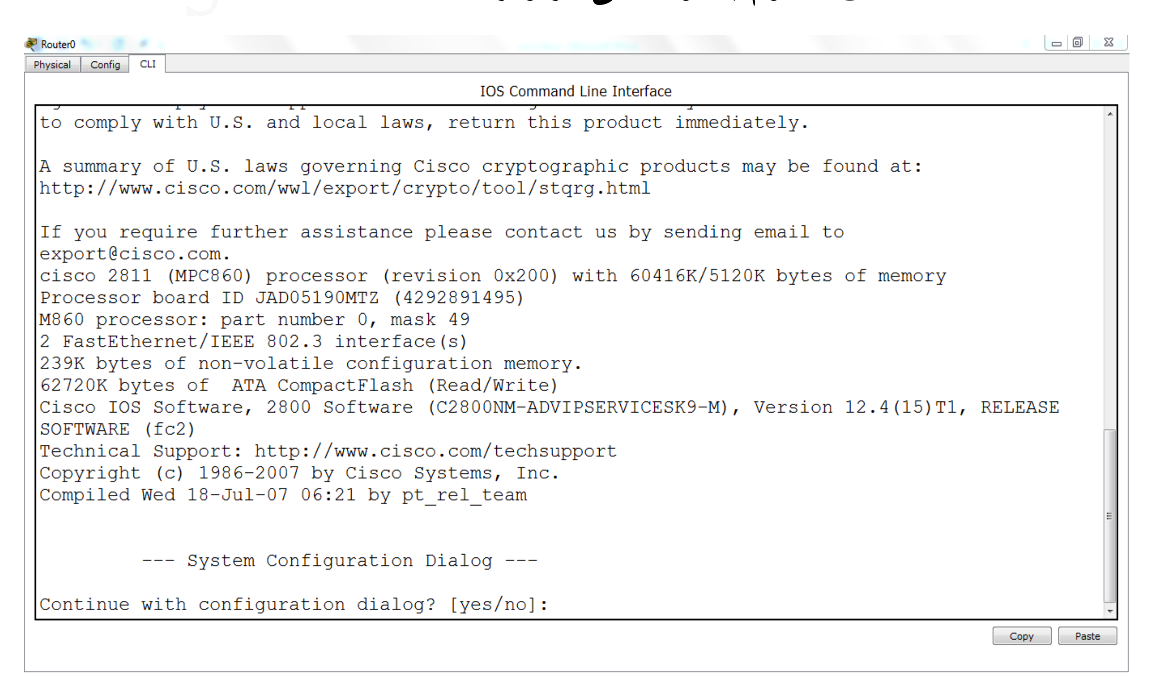
IP: 10.0.0.0/8 عنوان الشبكة الثالثة.

GY: 10.0.0.1 هذا الاي بي سيتم تركيبها على الإنترفيس **f0/1** الذي على الراوتر المسمى **Router 0**.

GY: 10.0.0.2 هذا الاي بي سيتم تركيبها على الإنترفيس **f0/1** الذي على الراوتر المسمى **Router 1**.

Mask: 255.0.0.0 عنوان قناع الشبكة على الراوترين.

الأن سنقوم بدخول على الراوتر **Router 0**



بعد الدخول على جهاز الراوتر قم بكتابة **No** لعملية الاستكمال ....

- الأن سنقوم بعملية اعداد الشبكة الأولى التي تاخذ عنوان اي بي **192.168.1.0/24**

الأن سنقوم بكتابة الاوامر التالية :

Router > **enable**

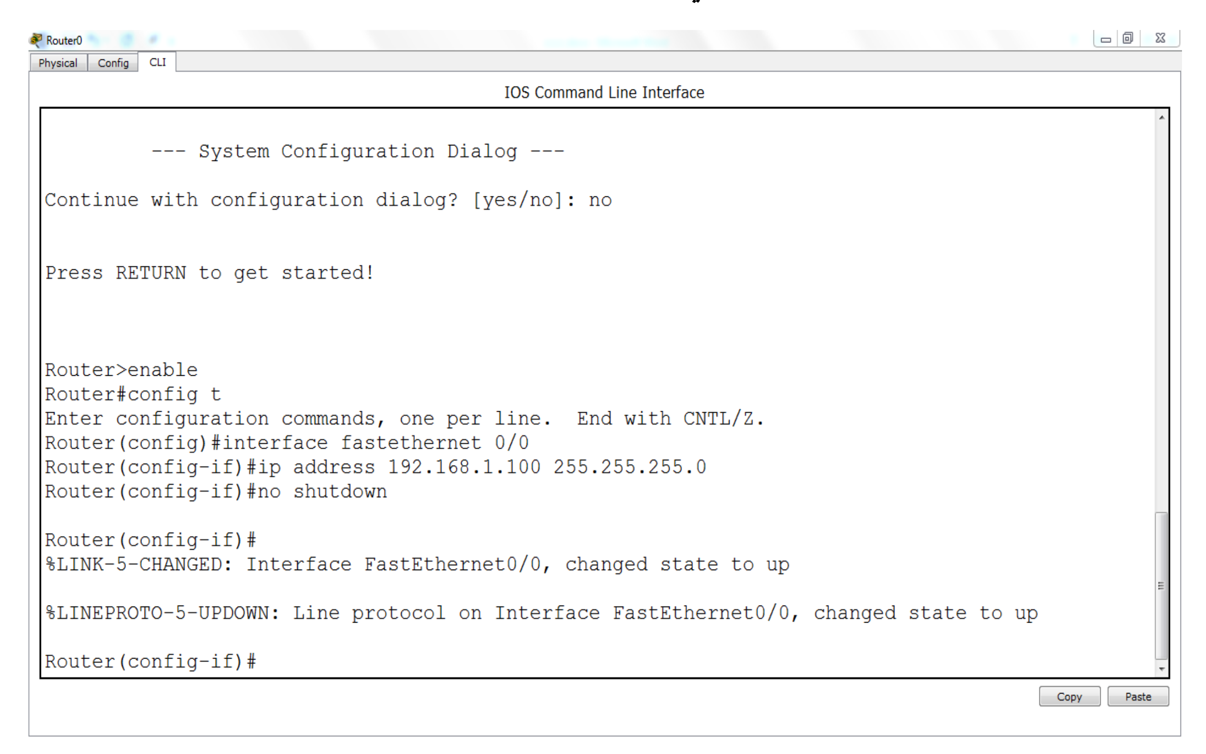
Router # **config t**

Router (config) # **interface fastethernet 0/0**

Router (config-if) # **ip address 192.168.1.100 255.255.255.0**

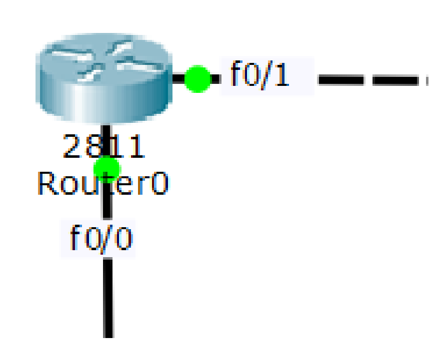
Router (config-if) # **no shutdown**

كما في الصورة التالية



- الأن تم تشغيل و تركيب الاي بي **192.168.1.100** على الإنترفيس **f0/0** .
- الأن سنقوم برجوع على المستوى السابق **exit** # Router (config-if) .
- الأن سنقوم بدخول على الإنترفيس **f0/1** و نقوم بتركيب الاي بي **10.0.0.1**.

هذا النموذج يوضح كل انترفيس تم ربطه في اية شبكة .



الأن سنقوم بكتابة الاوامر التالية :

Router > **enable**

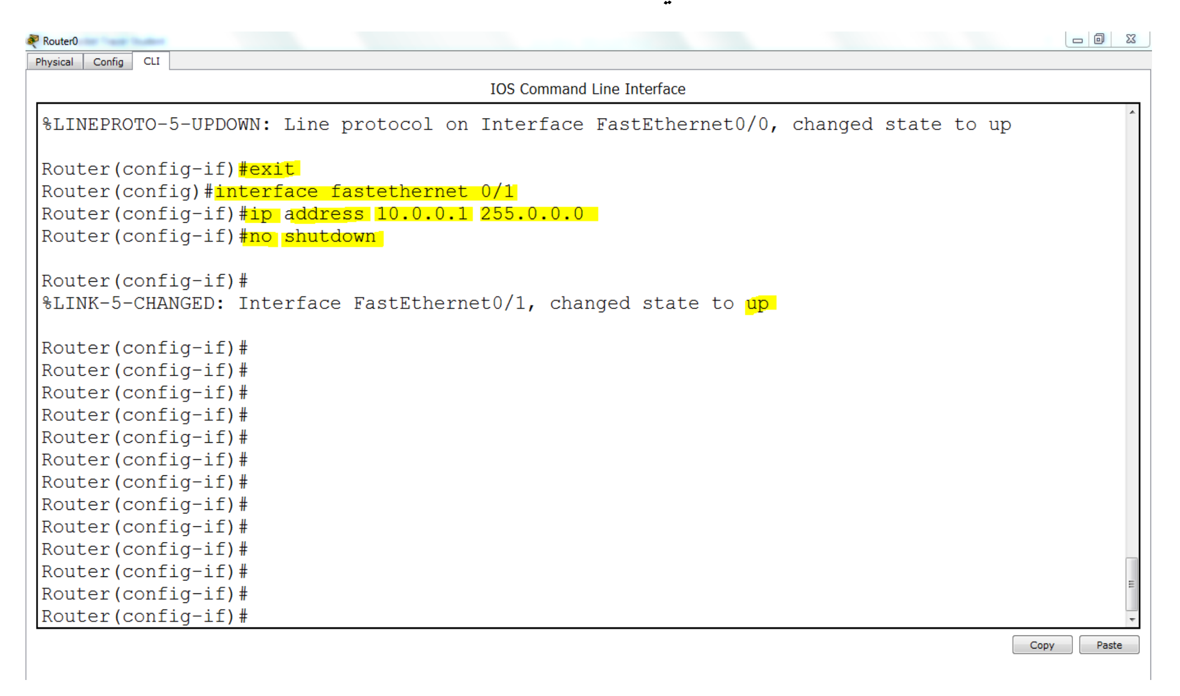
Router # **config t**

Router (config) # **interface fastethernet 0/1**

Router (config-if) # **ip address 10.0.0.1 255.0.0.0**

Router (config-if) # **no shutdown**

كما في الصورة التالية



```
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up

Router(config-if)#exit
Router(config)#interface fastethernet 0/1
Router(config-if)#ip address 10.0.0.1 255.0.0.0
Router(config-if)#no shutdown

Router(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to up

Router(config-if)#
Router(config-if)#
Router(config-if)#
Router(config-if)#
Router(config-if)#
Router(config-if)#
Router(config-if)#
Router(config-if)#
Router(config-if)#
Router(config-if)#
Router(config-if)#
Router(config-if)#
Router(config-if)#
```

- الأن تم تشغيل و تركيب الاي بي **10.0.0.1** على الإنترفيس **f0/1** .
- الأن سنقوم بالخروج على المستوى السابق Router (config-if) # **end** .
- الأن سنقوم بعملية حفظ الإعدادات و نقلها من ذاكرة الـ **RAM** إلى ذاكرة الـ **NVRAM**.
- Router # **copy running-config startup config**

```
Router#
Router#
Router#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
Router#
```

- بهذه الطريقة قمنا بعمل إعدادات الراوتر المسمى **Router 0** تم تشغيل الإنترفيس **f0/0** للشبكة **192.168.1.0/24** و تم تشغيل الإنترفيس **f0/1** للشبكة الثالثة

10.0.0.0/8 و بهذه الطريقة نكون قد تم اعداد الراوتر بشكل صحيح الأن ننتقل للراوتر المسمى Router 1 و سنقوم بتشغيل الإنترفيس و تركيب الاي بي على كل انترفيس.

الأن سنقوم بدخول على الراوتر Router 1

بعد الدخول على جهاز الراوتر قم بكتابة **No** لعملية الاستكمال ....

- الأن سنقوم بعملية اعداد الشبكة الثانية التي تاخذ عنوان اي بي **192.168.2.0/24**

Router > **enable**

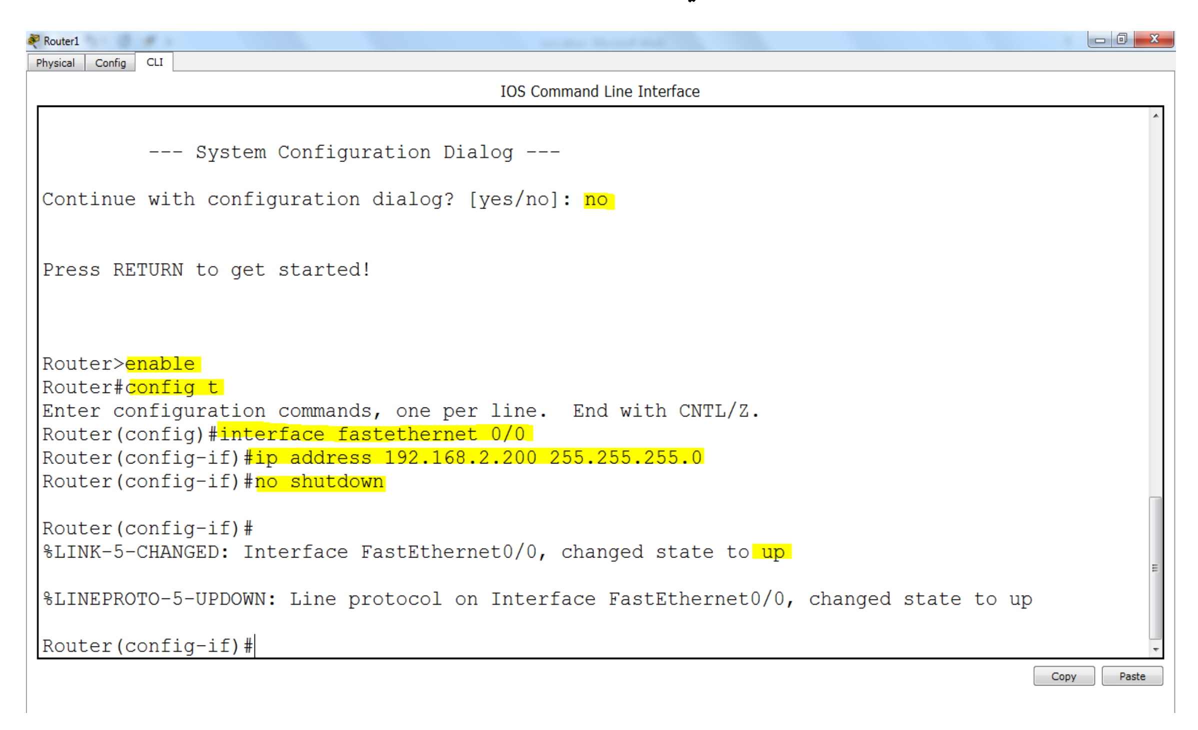
Router # **config t**

Router (config) # **interface fastethernet 0/0**

Router (config-if) # **ip address 192.168.2.200 255.255.255.0**

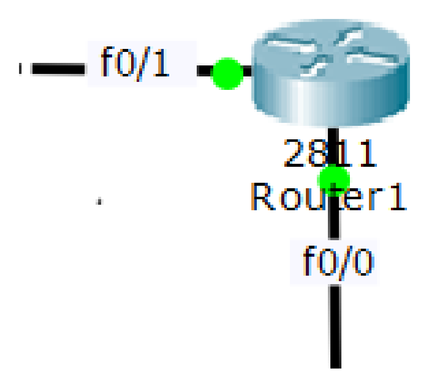
Router (config-if) # **no shutdown**

كما في الصورة التالية



- الأن تم تشغيل و تركيب الاي بي **192.168.2.200** على الإنترفيس **f0/0** .
- الأن سنقوم برجوع على المستوى السابق **exit** # Router (config-if) .
- الأن سنقوم بدخول على الإنترفيس **f0/1** و نقوم بتركيب الاي بي **10.0.0.2**.

- **هذا النموذج يوضح كل انترفيس تم ربطه في اية شبكة .**



الأن سنقوم بكتابة الاوامر التالية :

Router > **enable**

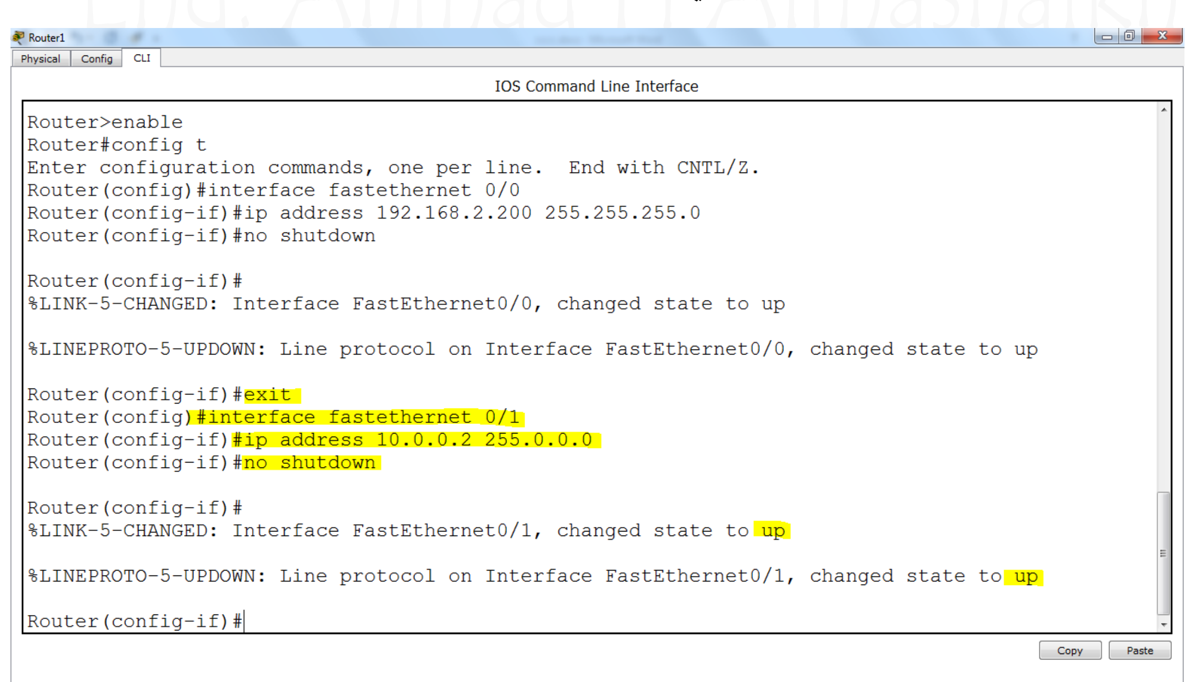
Router # **config t**

Router (config) # **interface fastethernet 0/1**

Router (config-if) # **ip address 10.0.0.2 255.0.0.0**

Router (config-if) # **no shutdown**

كما في الصورة التالية



- الأن تم تشغيل و تركيب الاي بي **10.0.0.2** على الإنترفيس **f0/1** .
- الأن سنقوم بالخروج على المستوى السابق **end** # Router (config-if) .
- الأن سنقوم بعملية حفظ الإعدادات و نقلها من ذاكرة الـ **RAM** إلى ذاكرة الـ **NVRAM**.
- Router # **copy running-config startup config**

```
Router#
Router#
Router#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
Router#
```

- بهذه الطريقة قمنا بعمل إعدادات الراوتر المسمى **Router 1** تم تشغيل الإنترفيس **f0/0** للشبكة **192.168.2.0/24** و تم تشغيل الإنترفيس **f0/1** للشبكة الثالثة **10.0.0.0/8** و بهذه الطريقة نكون قد تم اعداد الراوتر بشكل صحيح.

- بهذه الطريقة قمنا بعملية إعدادات تشغيل الإنترفيس لجميع الراوترات و تم تركيب العناوين على جميع الإنترفيس و بهذه الطريقة الشبكة الداخلية تعمل ولكن في هذه الحالة شبكة **192.168.1.0/24** لا تستيطع الاتصال بشبكة **192.168.2.0/24** في هذه الحالة نحتاج للشبكة الثالثة **10.0.0.0/8** و هي التي ستقوم بربط ما بين الشبكة الأولى و الشبكة الثانية لتتمكن من الاتصال ببعضهما البعض و يستطيعون تبادل المعلومات و البيانات في ما بينهم الأن سنحتاج لعمل التوجيه اليدوي **Static Routing** و عمل التوجيه و تعريف الشبكات في كل راوتر لتتم عملية الاتصال في جميع الشبكات نبداء في إعدادات التوجيه اليدوي .

- قبل أن نبداء يجب أن نتعرف على بعض الاوامر المهمة جداً جداً في عملية صيانة الشبكات :

Router # **show ip interface brief**

هذا الأمر يستخدم لعرض جميع المنافذ الموجودة في جهاز الراوتر مع جميع عناوين الاي بي الموجودة على الروترات و حالتها هل هي تعمل أو لا **Up or Down**

Router # **show ip route**

هذا الأمر يستخدم لعرض جدول التوجيه في الراوتر و الشبكات المتصلة في الراوتر

Router # **show ip protocol**

هذا الأمر يستخدم لعرض البروتوكولات المستخدمة في جهاز التوجيه الراوتر

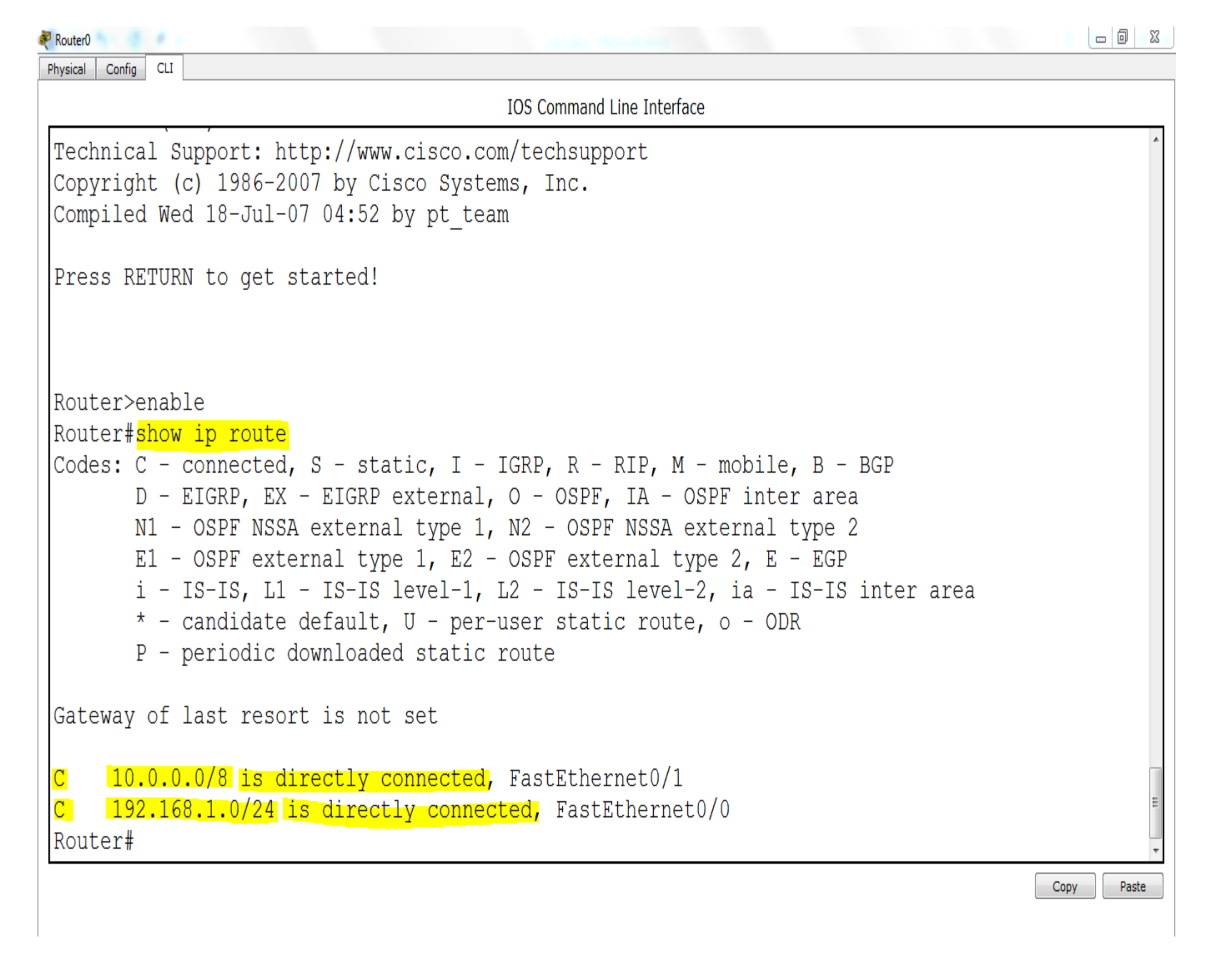
Router # **show running-config**

هذا الأمر يستخدم لمعرفة تفاصيل ملف الإعدادات يحتوي على جميع التفاصيل التي تعمل في الجهاز .

- سنقوم بدخول على الراوتر المسمى **Router 0** و سنقوم بعملية عرض جدول التوجيه الموجود في هذا الراوتر قبل أن نقوم بعملية إعدادات التوجيه اليدوي يفضل أن نقوم بهذه الامور قبل أن نبداء في تعريف و إضافة الشبكة لكي لا يحدث اية مشاكل في الشبكة و نقوم بكتابة الأمر التالي :

Router # **show ip route**

كما في الصورة التالية Router 0



```
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2007 by Cisco Systems, Inc.
Compiled Wed 18-Jul-07 04:52 by pt_team

Press RETURN to get started!



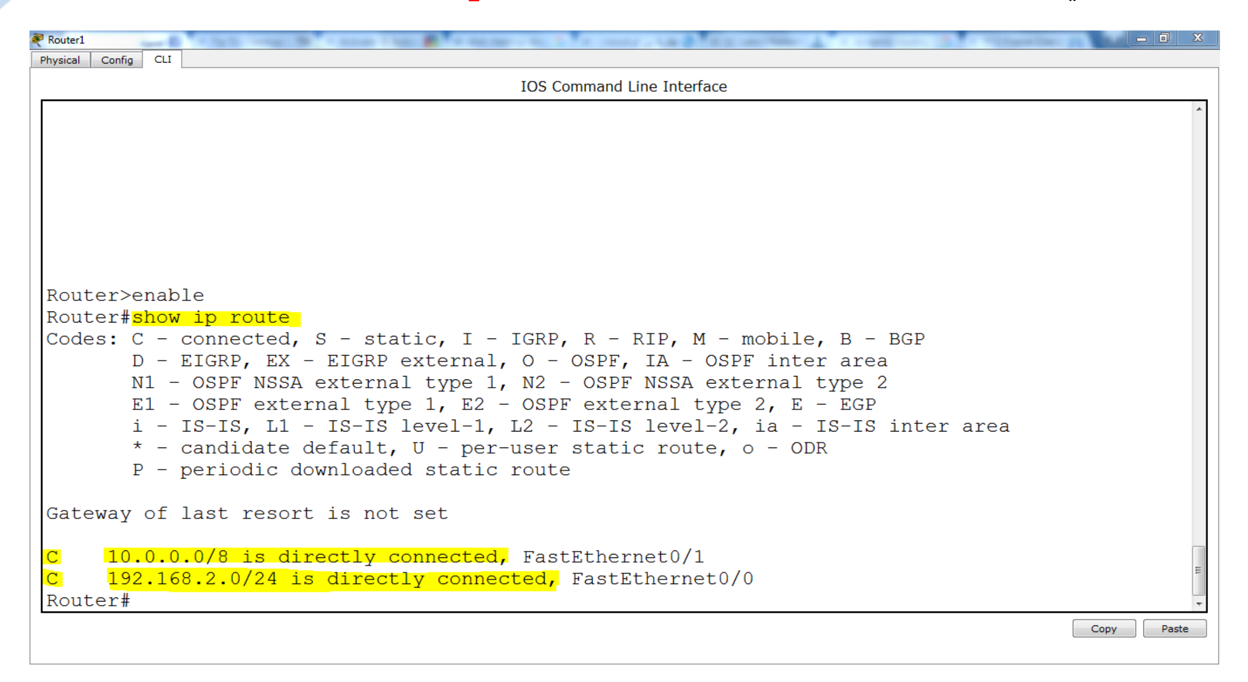
Router>enable
Router#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

C    10.0.0.0/8 is directly connected, FastEthernet0/1
C    192.168.1.0/24 is directly connected, FastEthernet0/0
Router#
```

- أنظر في هذه الصورة يظهر لدنيا شبكتين الشبكة **10.0.0.0/8** و الشبكة **192.168.1.0/24** يجب أن نعلم أن هذه الشبكات تم توصيلها بشكل مباشر و تاخذ الرمز " **C** " و هذا يدل على الاتصال المباشر في جدول التوجيه , لاحظ إنه لا يوجد شبكة بعنوان **192.168.2.0/24** نعم إنه لم يتم إضافة هذه الشبكة في جدول التوجيه و في هذه الحالة لا تستيطع الشبكتين الاتصال في بعض الا بعد أن نقوم بعمل التوجيه اليدوي ليتم الاتصال قبل أن نبداء في عملية الإعدادات يجب أن نتاكد هل الشبكة **192.168.1.0/24** موجودة في الراوتر المسمى **Router 1 أو** لا يجب أن نتاكد بدخول على الراوتر **Router 1** و نقوم بعرض جدول التوجيه و نتاكد سنقوم بكتابة الأمر التالي :

كما في الصورة التالية **Router 1** : Router # **show ip rout**



كما ظهر في الصورة لا وجود للشبكة **192.168.1.0/24** لإنه لم يتم عمل الإعدادات الخاص في التوجيه .

- الأن سنقوم بعملية إعدادات التوجيه اليدوي **Static Routing** نبداء :
- الأن نحن في الراوتر المسمى **Router 0** سنقوم بعمل الإعدادات التالية ....

الأن سنقوم بكتابة الاوامر التالية :

Router > **enable**

Router # **config t**

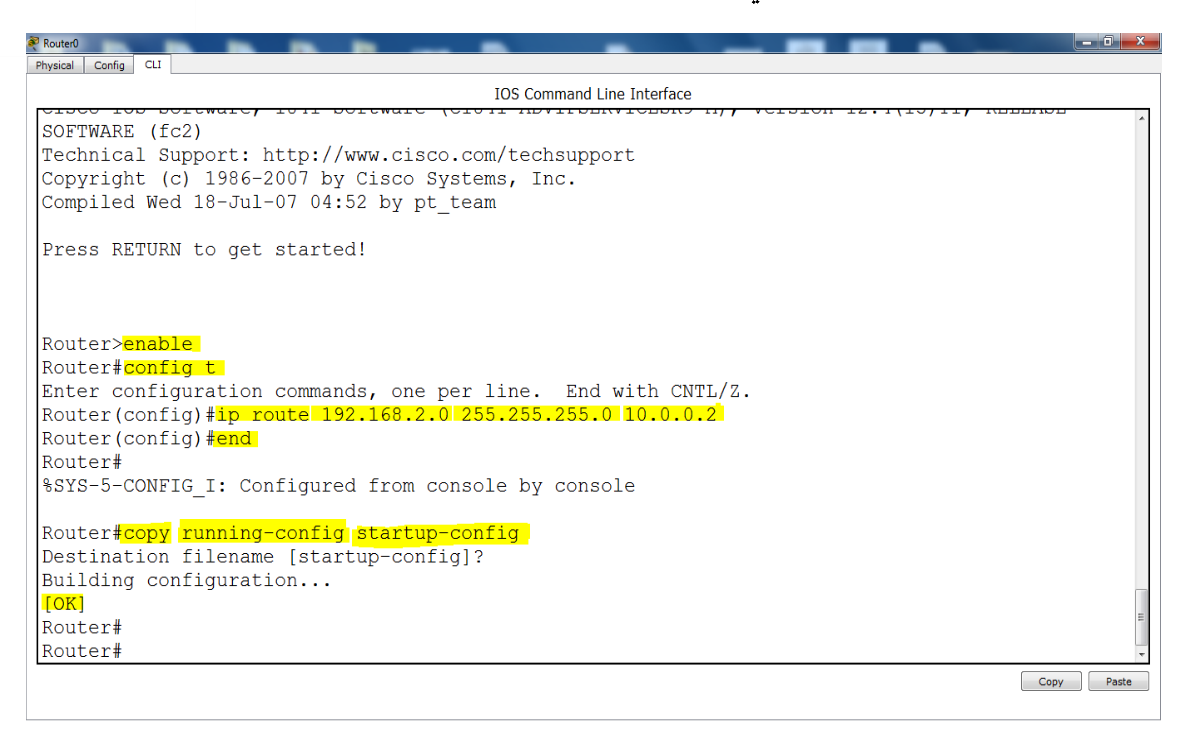
Router (config) # **ip route 192.168.2.0 255.255.255.0 10.0.0.2**

هذا الأمر يستخدم في التوجيه اليدوي فقط يقوم بعملية إضافة الشبكة المراد الاتصال فيه مع قناع الشبكة الخاص فيها و بعده تقوم بوضع اي بي الشبكة الثالثة **10.0.0.2** و هي الشبكة الوسيطة التي تربط ما بين الشبكتين **192.168.1.0/24** و **192.168.2.0/24** و بهذا الشكل سيتم الاتصال ما بينا الشبكات ولكن يجب أن نقوم بنفس هذه الخطوات على الراوتر الآخر المسمى **Router 1** .

Router (config) # **end**

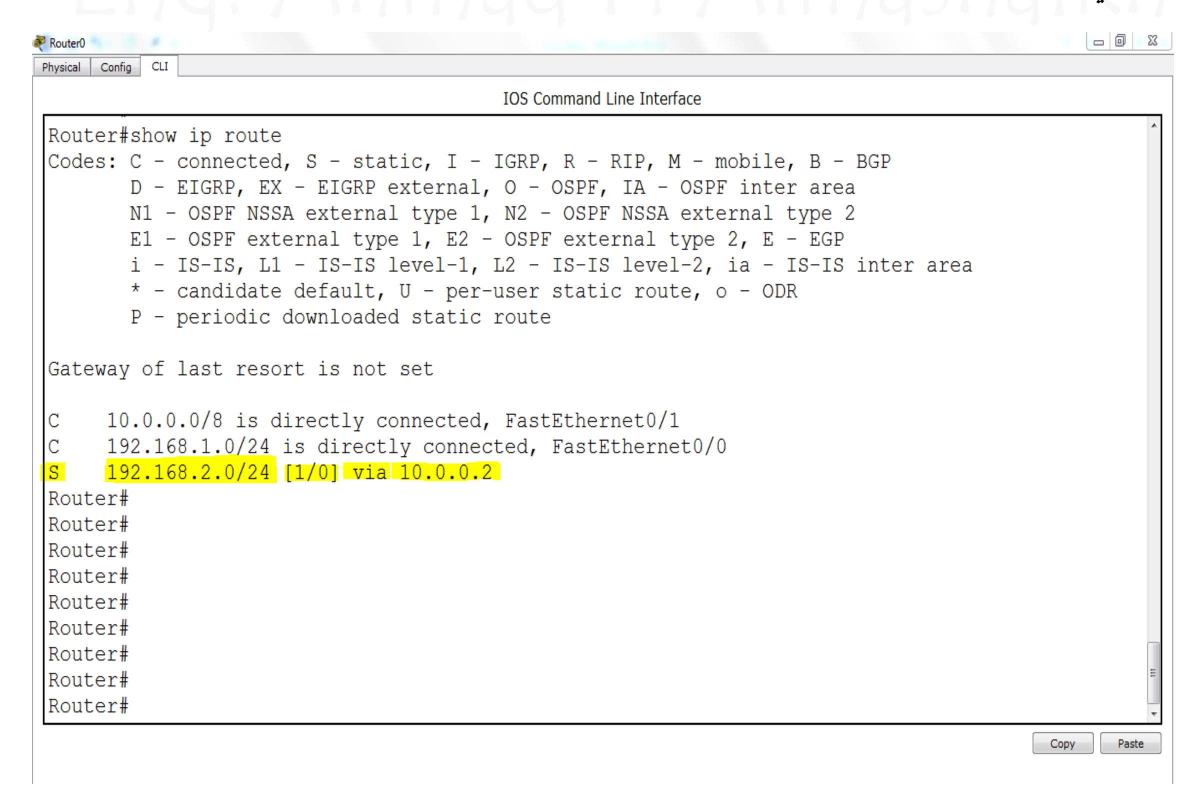
Router # **copy running-config startup-config**

كما في الصورة التالية Router 0



بعد عمل الخطوات السابقة سنقوم بكتابة الأمر التالي لعرض الشبكات لنتاكد هل تم إضافة الشبكة **192.168.2.0/24** أو لا . Router # **show ip route**

كما في الصورة التالية Router 0 :



- لاحظ إنه يوجد شبكة **192.168.2.0/24** و يتم الاتصال فيها عن طريق الشبكة **10.0.0.2/8** الأن في هذه الحالة تم إضافة الشبكة في جدول التوجيه اليدوي الخاص

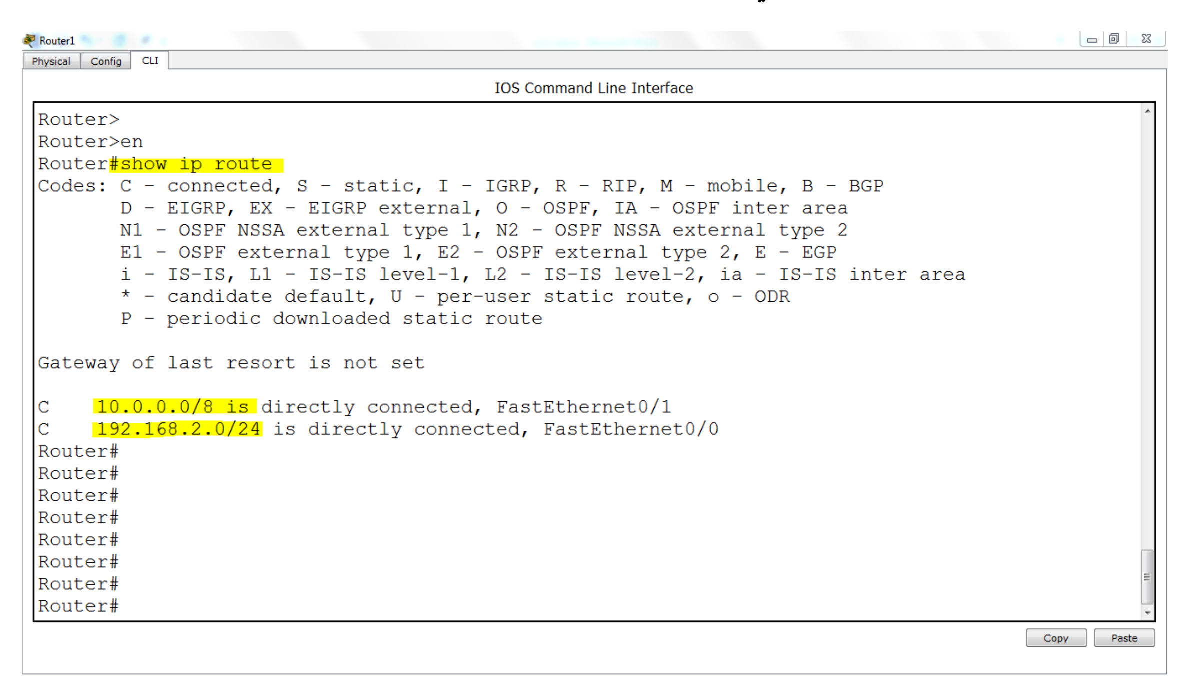
في راوتر **Router 0** سنقوم بنفس الإعدادات على الراوتر الآخر المسمى **Router1** و نقوم بعمل الإعدادات و إضافة الشبكة **192.168.1.0/24** في الراوتر الآخر .

- قبل الانتقال لجهاز الراوتر الآخر لاحظ إنه يوجد شيء ما بعد عنوان الشبكة **192.168.2.0/24 [1/0]** هذا هو الـ **Next Hop** عدد القفزات التي في المسار أنظر في الصورة السابقة عدد القفزات **[1/0]** قفزة واحد بمعنى إنه تم القفز عن انترفيس متصل في الراوتر موجود في المسار إذا كان اكثر من راوتر سيتم كتابة ما فوق الرقم واحد .

- سنقوم بدخول على الراوتر المسمى **Router 1** و سنقوم بعملية عرض جدول التوجيه الموجود في هذا الراوتر قبل أن نقوم بعملية إعدادات التوجيه اليدوي يفضل أن نقوم بهذه الامور قبل أن نبداء في تعريف و إضافة الشبكة لكي لا يحدث اية مشاكل في الشبكة و نقوم بكتابة الأمر التالي :

Router # **show ip route**

كما في الصورة التالية Router 1



كما ظهر في الصورة لا وجود للشبكة **192.168.1.0/24** لإنه لم يتم عمل الإعدادات الخاص في التوجيه .

- الأن سنقوم بعملية إعدادات التوجيه اليدوي **Static Routing** نبداء :
- الأن نحن في الراوتر المسمى **Router 1** سنقوم بعمل الإعدادات التالية ....

الأن سنقوم بكتابة الاوامر التالية :

Router > **enable**

Router # **config t**

Router (config) # **ip route 192.168.1.0 255.255.255.0 10.0.0.1**

Router (config) # **end**

Router # **copy running-config startup-config**

```
Router>enable
Router#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#ip route 192.168.1.0 255.255.255.0 10.0.0.1
Router(config)#end
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
Router#
Router#
```

بعد عمل الخطوات السابقة سنقوم بكتابة الأمر التالي لعرض الشبكات لنتاكد هل تم إضافة الشبكة **192.168.2.0/24** أو لا . Router # **show ip route**

كما في الصورة التالية Router 1

Router1
Physical | Config | CLI

IOS Command Line Interface

```
Destination filename [startup-config]?
Building configuration...
[OK]
Router#
Router#
Router#
Router#
Router#
Router#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

C    10.0.0.0/8 is directly connected, FastEthernet0/1
S    192.168.1.0/24 [1/0] via 10.0.0.1
C    192.168.2.0/24 is directly connected, FastEthernet0/0
Router#
```

Copy | Paste

- الأن بهذه الطريقة تم إعدادات جميع الشبكات و الأن نستطيع الاتصال في جميع الشبكات :

- شبكة **192.168.1.0/24** تستطيع الاتصال في شبكة **192.168.2.0/24** عن طريق شبكة **10.0.0.0/8** بهذه الطريقة نكون قد تم الانتهاء من هذه الشبكات الثالثة .
- سنقوم بعمل اختبار هل هذه الشبكة تتصل في بعضها البعض أو لا سنقوم بعمل الاتصال ما بين الراوترات و بعده سنقوم بدخول على الأجهزة و نقوم بعمل اختبار من داخل الشبكة عن طريق الأمر **Ping** تابع .
- سنقوم بعمل اتصال ما بين الراوتر أولاً عن طريق الأمر **Ping** كما هو موجود في الصورة التالية :

Router 0 قام بعمل **Ping** على الشبكة **10.0.0.2** الموجودة على **Router 1** لاحظ تم الرد عليه **Success** هذا يعني إنه تم الاتصال بشكل صحيح لأن عملية الـ **ping** تتكون من **packet 5** أنظر في هذه الصورة تم وصول **packet 4** تم اسقاط **packet** واحدة.

و قمنا ايضاً بعمل **ping** على الشبكة الثانية **192.168.2.200** لاحظ وصول الـ **packet** بشكل كامل و عد تقطع في الوصول لقد تم وصول **5 packet** للشبكة **192.168.2.200** بشكل صحيح أنظر في الصورة اسفل :

Router 0

```
Router0
Physical  Config  CLI
IOS Command Line Interface

Copyright (c) 1986-2007 by Cisco Systems, Inc.
Compiled Wed 18-Jul-07 04:52 by pt_team

Press RETURN to get started!


Router>enable
Router#ping 10.0.0.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.0.2, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 0/0/0 ms

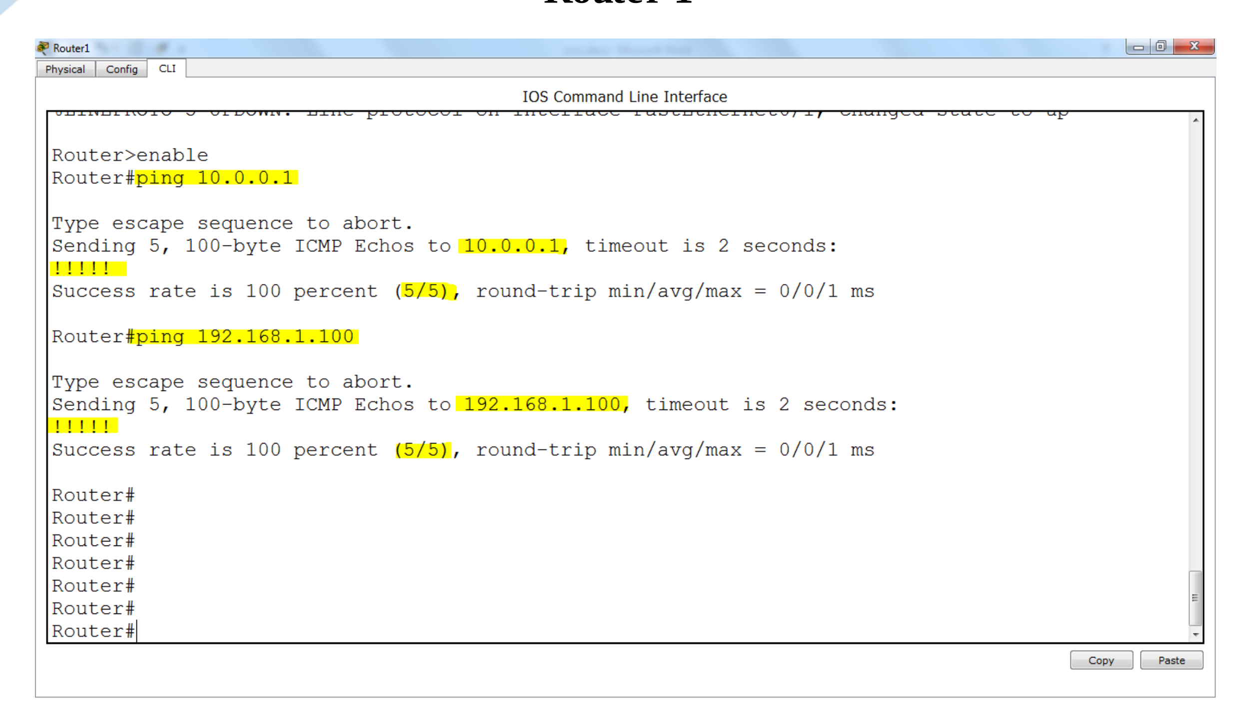
Router#ping 192.168.2.200

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.2.200, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/2 ms

Router#
Copy  Paste
```

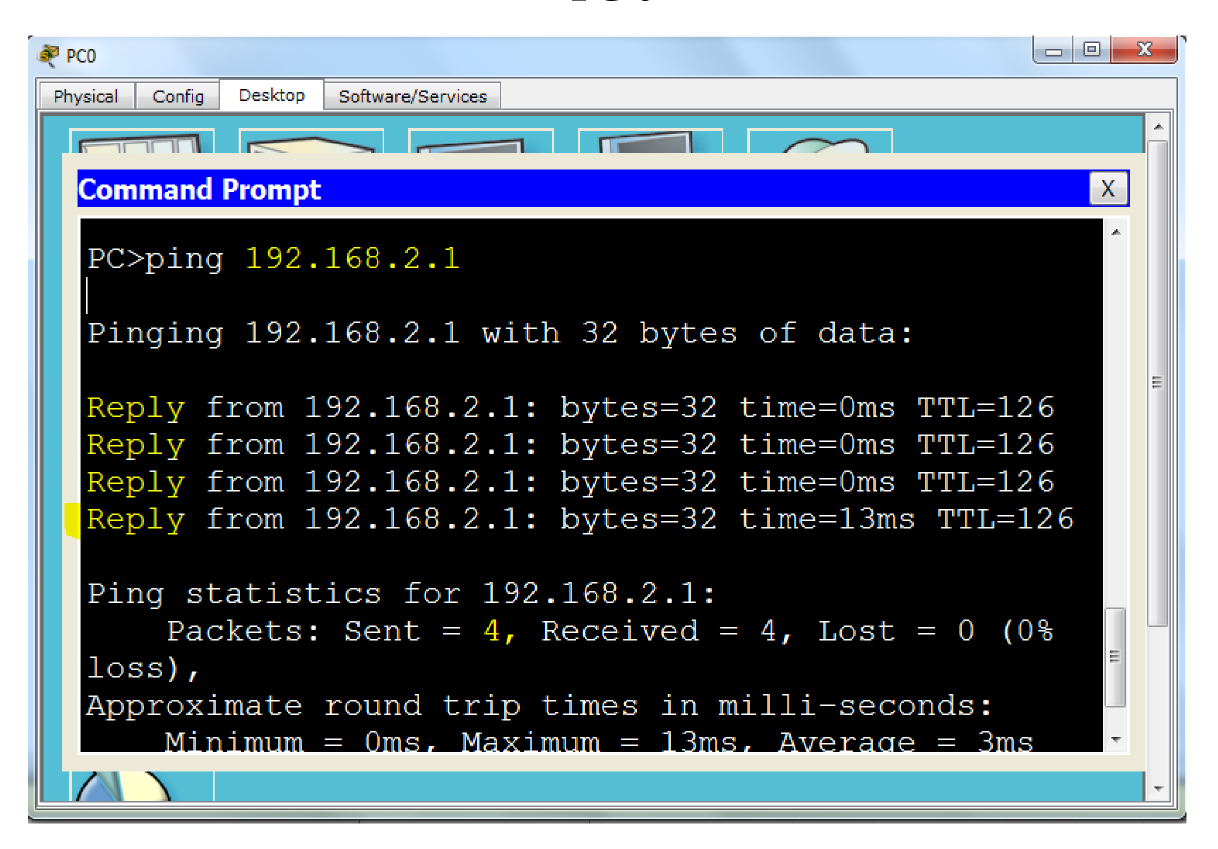
- راوتر الثاني أنظر ايضاً يستطيع أن يتصل في الشبكات الآخر الموجودة في راوتر **Router 0** كم في الصورة التالية :

Router 1



- الأن سنقوم بعملية الـ **ping** من جهاز الحاسوب **PC 0** الموجود في شبكة **192.168.1.1** و نريد أن نقوم بعملية الـ **ping** على جهاز الحاسوب **PC 1** الموجود في شبكة **192.168.2.1** كم هو موجود في الصورة التالية :

PC 0



- لاحظ تم الرد من جهاز الحاسوب **PC 1** الموجود في شبكة **192.168.2.1** تم الرد بي **4 packet** بشكل كامل .

- الأن سنقوم بعملية الـ **ping** من جهاز الحاسوب **PC 1** الموجود في شبكة **192.168.2.1** و نريد أن نقوم بعملية الـ **ping** على جهاز الحاسوب **PC 0** الموجود في شبكة **192.168.1.1** كم هو موجود في الصورة التالية :

```
PC1
Physical | Config | Desktop | Software/Services
Command Prompt
    Packets: Sent = 4, Received = 2, Lost = 2 (50%
loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

PC>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

Reply from 192.168.1.1: bytes=32 time=0ms TTL=126
Reply from 192.168.1.1: bytes=32 time=0ms TTL=126
Reply from 192.168.1.1: bytes=32 time=0ms TTL=126
Reply from 192.168.1.1: bytes=32 time=2ms TTL=126

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 2ms, Average = 0ms

PC>
```

- لاحظ تم الرد من جهاز الحاسوب **PC 0** الموجود في شبكة **192.168.1.1** تم الرد بي **4 packet** بشكل كامل .

هاكذا نكون قد تم الانتهاء من درس **Static Routing** .

بعض الاوامر المهمة و الملاحظات يوجد امر مهم جداً جداً جداً يجب أن نعرفه و ناخذ الحذر منه و نفهم ماذا سيفعل .

- **في حال نريد إضافة شبكة عن طريق الـ Static Routing نقوم بكتابة الأمر التالي**

Router (config) # **ip route 192.168.1.0 255.255.255.0 10.0.0.1**

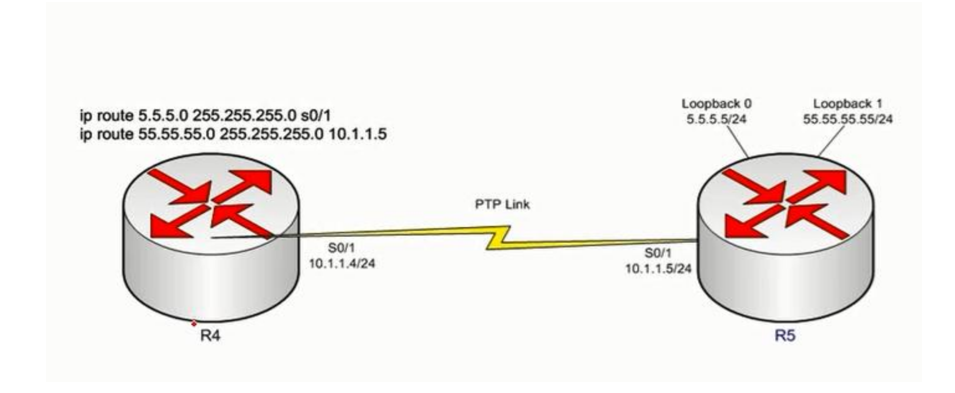
- هذا الأمر الذي قمنا بعمل الإعدادات به و يعتمد على عنوان الشبكة و يوجد امر ثاني يعتمد على الإنترفيس المتصل في الشبكة بدل من كتابة الاي بي و سأقوم بتفريق ما بينهم .

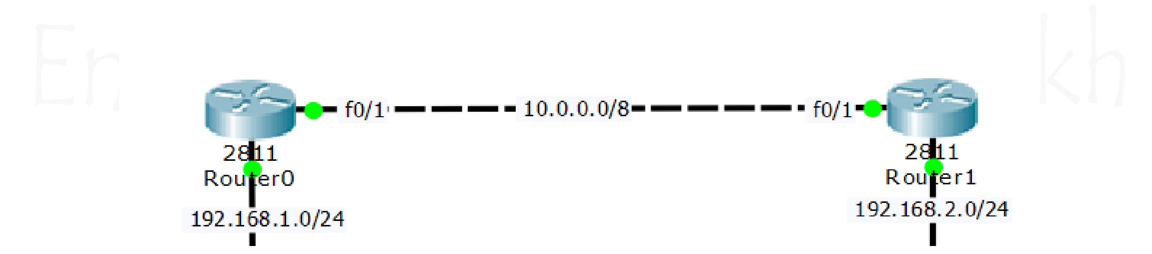
Router (config) # **ip route 192.168.1.0 255.255.255.0 10.0.0.1**

Router (config) # **ip route 192.168.1.0 255.255.255.0 f0/1**

- لاحظ إنه الأمر الثاني متصل من الإنترفيس و معتمد على الإنترفيس على عكس الأمر الأول الذي يعتمد على الاي بي في هذه الحاله إذا تم العمل و الاعتماد على كتابة الإنترفيس في هذه الحالة سيتم الاتصال بشكل مباشر ولا يقوم بعد عدد القفزات الإنه الاتصال مباشر على عكس وضع الاي بي الذي يعد عدد القفزات .

كما في الصورة التالية توضح الفرق ايضاً ولكن في هذه الصورة تم الربط بكابل السيريل.





Dynamic Routing IPv4

التوجيه الأوتوماتيكي و البروتوكولات التي تعمل فيه

بروتوكول مسار المعلومات

RIP = Routing Information Protocol

RIP : هوبروتوكول مسار المعلومات و يصنف كبروتوكول بوابة داخلية **IGP** و يستخدم ايضاً من خوارزميات التوجيه و خوارزمية المسافة و تم توسيعه عدة مرات، و أدى ذلك لإنتاج الإصدار عدة اصدارات و كان الإصدار المطور من بروتوكول الـ **RIP** هو الإصدار الثاني.

الإصدار الثاني هو **RIP2** و في الإصدارين ما يزالأن قيد الاستخدام في أيامنا هذه، على الرغم من ظهور تقنيات أكثر تقدماً مثل تقنية (فتح أقصر مسار أولاً **OSPF**) و بروتوكول **IS-IS** كما تم إصدار نسخة من بروتوكول الـ **RIP** متأقلمة مع البروتوكول **IPv6** و هي المعيار المعرف ببروتوكول **RIP** (**RIPng** الجيل الثالث) الذي تم رفعه عام **1997**.

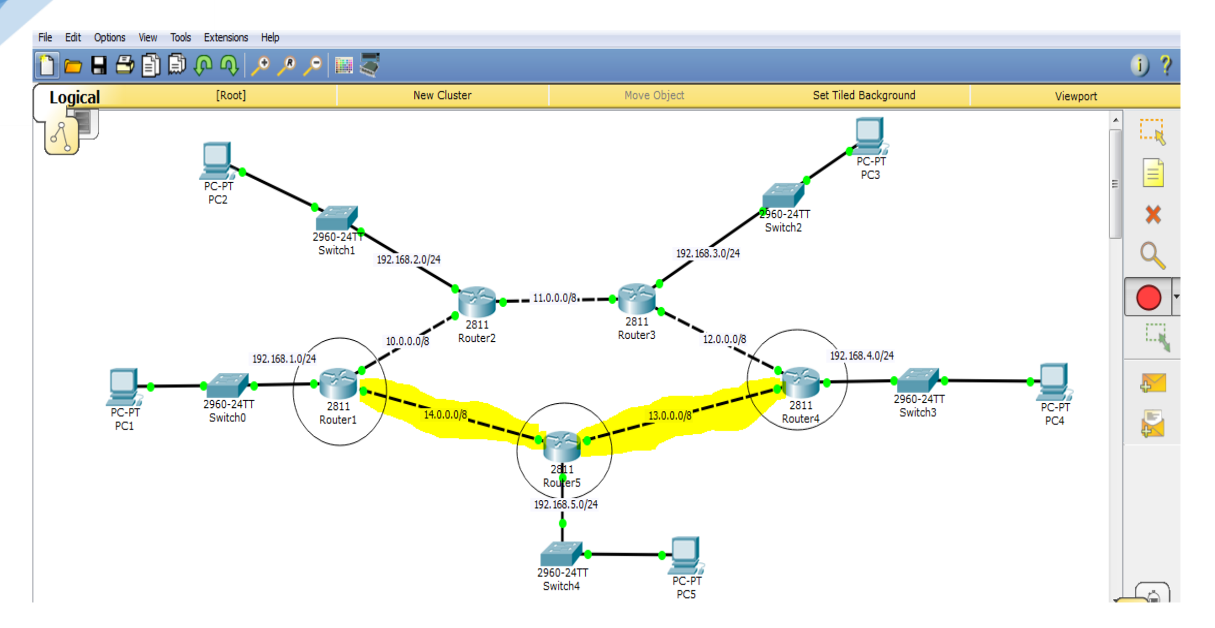
لمحة تاريخية : إن خوارزمية التوجيه المستخدمة في بروتوكول **RIP** و التي تدعى بخوارزمية(**Bellman-Ford**) أو خوارزمية شعاع المسافة كان أول انتشار لها في شبكة الحاسب عام **1967** كخوارزمية التوجيه الأولية من **ARPANET** .

تفاصيل تقنية RIP: هو عن بروتوكول توجيه شعاع المسافة، و الذي يوظف عداد خطوات كمقياس للتوجيه. و لتجنب مشكلة العد إلى ما لا نهاية قام بروتوكول الـ **RIP** بتعريف عدد أقصى للمسافة و هي (عدد الخطوات) المسموح بها من المصدر إلى الوجهة. فالعدد الاقصى للخطوات المسموح بها هو **15** في بروتوكول.**RIP** و هذا العدد المحدود أيضاً يقوم بتحديد حجم الشبكات التي يمكن لبروتوكول الـ **RIP** أن يدعمها. تم بناء **RIP** فوق بروتوكول **UDP** كبروتوكول النقل الخاص به. و يعمل على البوابة رقم **520** الإصدارات.

- هذا البروتوكول يعمل في البطقة السابعة و هي طبقة التطبيقات **Application Layer** .
- هذا البروتوكول يستخدم و يعتمد على خوارزمية أقصر مسار **Distance Vector Protocol** .
- يعمل باستخدام جدول واحد و هو جدول التوجيه الذي يتم فيه تسجيل عناوين الشبكات و المسارات **Routing Table**.
- قيمة المسافة الإدارية لـ بروتوكول الـ **RIP** هي **120** .
- يقوم بحسب طريقة افضل مسار (**Metric**) عن طريق الـ **Hop Count** المسار صاحب عدد الراوترات الاقل الموجودة في المسار .
- يدعم هذا البروتوكول عدد اقصى **15** راوتر في الشبكة الواحدة فقط .
- يقوم بروتوكول الـ **RIP** بإرسال التحديثات كل ثلاثين ثانية و هو عبارة عن إرسال كامل جدول التوجيه .

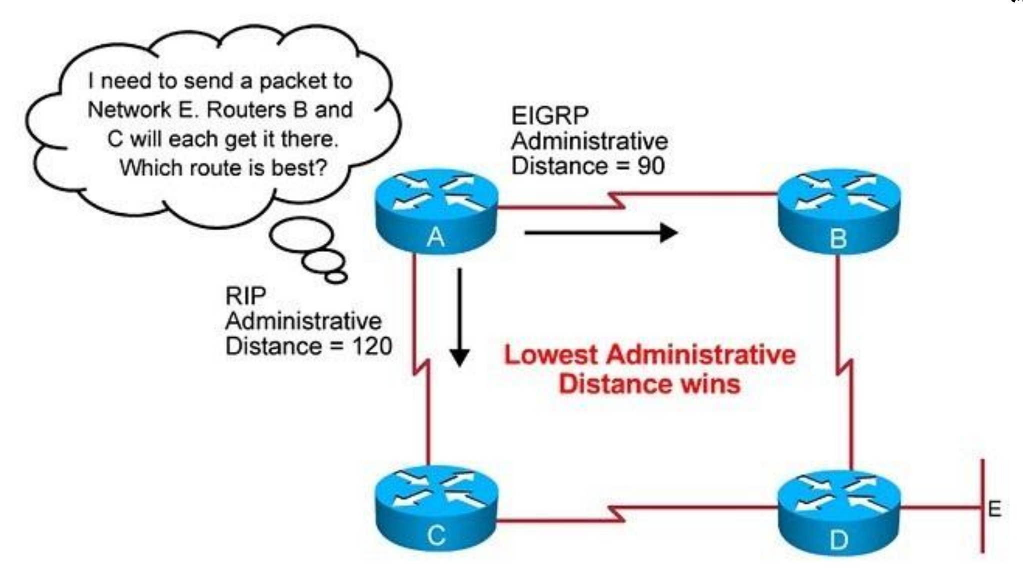
- **Distance Vector :** هذه خوارزمية اقصر مسار بمعنى عدد الراوترات التي في المسار مثل عندما ترسل البيانات ستقوم بدخول في المسار و ستبقى مرسلة للتوقف على آخر مسار في الشبكة و بنسبه لبروتوكول الـ **RIP** فقط يدعم **15** من عدد القفزات **15** قفزة فقط و عند وصول البيانات للقفزة رقم **15** سيقوم المستقبل باخذه و بعده سيتم الغاء البيانات لإنه لا يمكن تجاوز اكثر من **15** قفزة **Hop Count** .

- بروتوكول الـ **RIP** لا يهتم في سرعة المسار بلا يهتم في عدد القفزات و عدد الراوتر الموجودة في المسار و طبعاً عدد الراوترات في المسار الاقل سيقوم بإرسال البيانات منها مثال على ذالك النموذج التالي هذه شبكة مفعل عليه بروتوكول **RIP** , أنظر عليها و قم بتدقيق فيه ....



- بعد أن قمت بنظر على النموذج عليك الأن أن تعرف إنه إذا ارادة جهاز **PC 1** الموجود في شبكة **192.168.1.0/24** يريد أن يرسل بيانات لجهاز موجود في شبكة **192.168.4.0/24** للجهاز **PC 4** برايك اية مسار سيختار لعملية إرسال البيانات ؟ من الطبيعي سيقوم باختير المسار الذي تم تحديده بلون الاصفر لي إنه يحتوي على راوتر واحد في المسار بينما المسار الثاني يحتوي على راوترين في المسار , في هذه الحالة سيتم اختيار المسار صاحب عدد الراوتر الاقل .

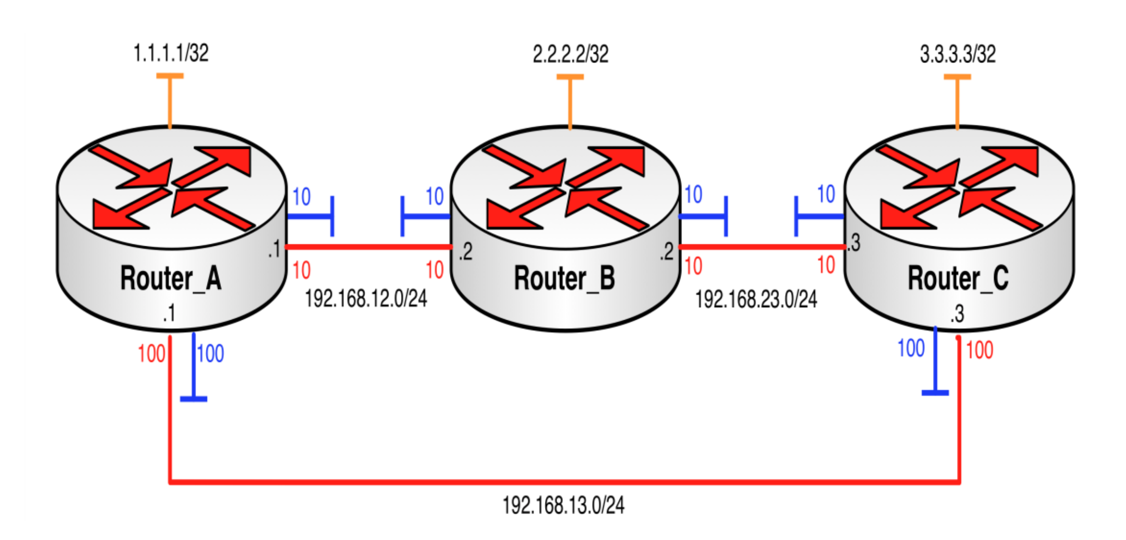
- **قيمة المسافة الإدارية Administrative distance** : هو الرقم الأول الذي يتم من خلاله تحديد المسار الذي سيتم الاعتماد عليه بين عدة مسارات للوصول إلى الشبكة المطلوبة حيث أن المسار صاحب الـ **Administrative distance** الاقل هو الذي سيصبح المسار المعتمد ، لكل **Routing protocol** الـ **Administrative distance** الخاص به اي عند امكانية الوصول إلى شبكة معينة باستخدام اكثر من بروتوكول فيتم استخدام البروتوكول صاحب ال **AD** الاقل ولكل بروتوكول قيمة مسافة ادارية مختلفة.



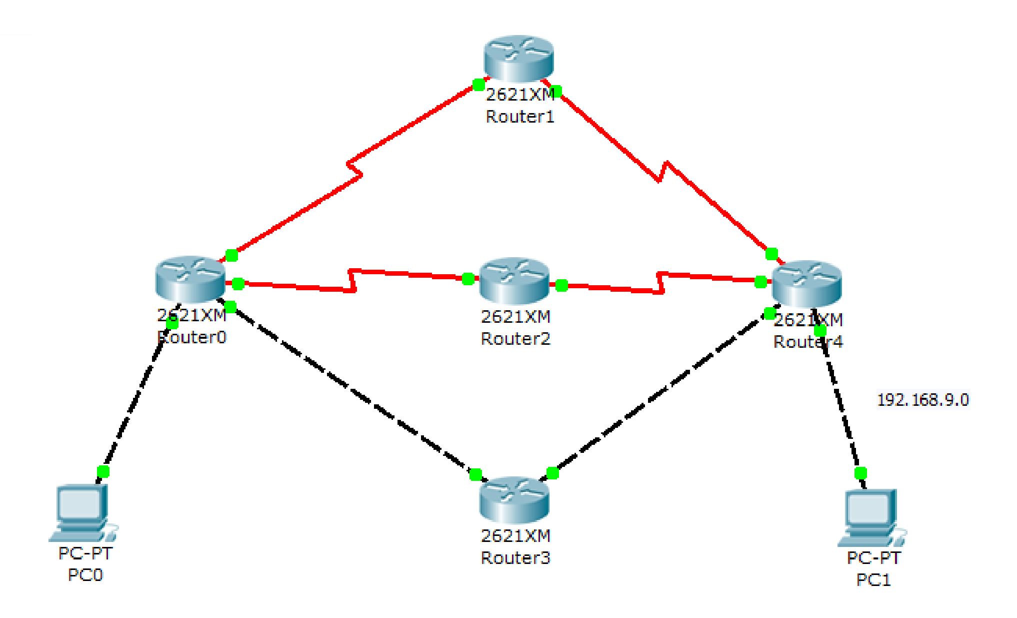
- وهذا الجدول يوضح قيم الـ **Administrative distance** في كل حالة .

Route Source	Default Distance	Routing Table Entry
Connected interface	0	C
Static route out an interface	0	S
Static route to a next-hop address	1	S
EIGRP summary route	5	D
External BGP	20	B
Internal EIGRP	90	D
IGRP	100	I
OSPF	110	O
IS-IS	115	i
RIPv1, RIPv2	120	R
Exterior Gateway Protocol (EGP)	140	E
ODR	160	O
External EIGRP	170	D EX
Internal BGP	200	B
Unknown	255	

Metric : هو الرقم الثاني الذي يتم الاعتماد عليه للوصول إلى الشبكة المطلوبة في حالة تساوي ال **AD** للمسارين ويتم تحديد قيمة ال **metric** في كل بروتوكول بطريقه مختلفة عن الآخر ففي ال **RIP** تكون قيمة ال **metric** هي عدد الراوترات التي يتم عبورها للوصول إلى الشبكة المطلوبة ، وفي ال **EIGRP** يتم استخدام الـ **Bandwidth**, **Delay**, **Reliability**, **Load** ووفق معادلة معينة يتم حساب الـ **metric** , وفي ال **OSPF** يتم حسابه عن طريق الـ **bandwidth** وهكذا ، وكما في الـ **AD** يتم اعتماد المسار صاحب الـ **metric** الاقل.



هذا نموذج شبكة نريد أن نعرف قيمة المسافة الإدارية :



- هذه الشبكة تم التطبيق فيه بروتوكولات الـ **EIGRP** و الـ **RIP** على جميع الراوترات وطبقنا الأمر **show ip route** على ال **Router 0** ستظهر النتيجة كالتالي :

```
Router#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route
                              administrative distance
Gateway of last resort is not set
                                                       metric
C    192.168.1.0/24 is directly connected, FastEthernet0/0
C    192.168.2.0/24 is directly connected, FastEthernet0/1
C    192.168.3.0/24 is directly connected, Serial1/1
C    192.168.4.0/24 is directly connected, Serial1/0
D    192.168.5.0/24 [90/20517120] via 192.168.1.2, 00:03:14, FastEthernet0/0
D    192.168.6.0/24 [90/20517120] via 192.168.1.2, 00:03:16, FastEthernet0/0
D    192.168.8.0/24 [90/30720] via 192.168.1.2, 00:03:21, FastEthernet0/0
D    192.168.9.0/24 [90/33280] via 192.168.1.2, 00:03:21, FastEthernet0/0
```

- لاحظ أن الـ **RIP** غير ظاهر في الـ **Table** وذلك لإنه يمتلك **AD** اعلى من الـ **EIGRP** فتم تجاهله والاعتماد على الـ **EIGRP** فقط ، وكذلك نلاحظ أن الشبكة **192.168.9.0** تم اعتماد مسار واحد لها رغم إنه في الحقيقة توجد **3** مسارات ، وذلك لأن الراوتر اعتمد المسار صاحب ال **metric** الاقل .

اذن الاعتماد على الـ **AD** أولا وفي حالة التساوي يتم اللجوء إلى الـ **metric**

- **ملاحظة هذا النموذج فقط ، منقول من أحد المواقع على شبكة الانترنت و أن قمت باخذه لتقليل الوقت في عمل الكتاب .**

- إصدارات بروتوكول الـ RIP (RIPv1 , RIPv2 , RIPng) هذه الإصدارات :

الإصدار الأول RIPv1	الإصدار الثاني RIPv2
يعمل بخوارزمية أقصر مسار	يعمل بخوارزمية أقصر مسار
العدد الأقصى للراوترات هو 15 راوتر	العدد الأقصى للراوترات هو 15 راوتر
قيمة المسافة الإدارية 120	قيمة المسافة الإدارية 120
لا يدعم تقسيم الشبكة	يدعم تقسيم الشبكة
يعمل باستخدم عنوان البث المباشر 255.255.255.255	يعمل باستخدم عنوان البث المباشر 224.0.0.9
لا يدعم كلمة المرور أو التشفير	يدعم كلمة المرور مع التشفير

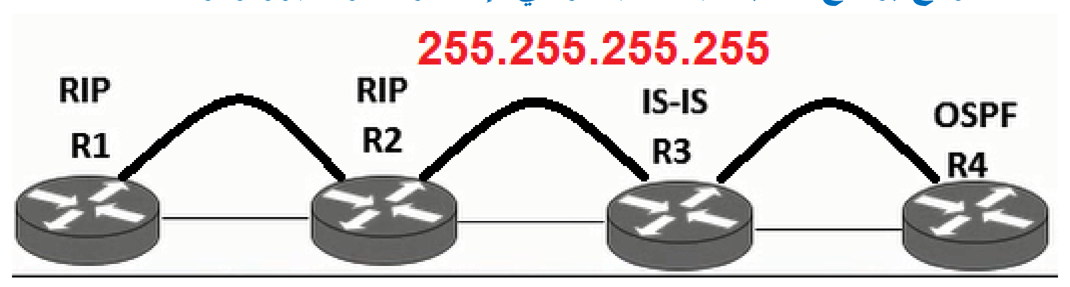
- عنوان البث المباشر الذي يتواجد في بروتوكول RIPv1
- الإصدار الأول 255.255.255.255 لديه عيوب كثيرة مثل عندما يكون لدينا اكثر من راوتر في الشبكة على سبيل المثال 4 راوترات و من هذه الـ 4 راوتر تم تفعيل بروتوكول الـ RIPv1 على راوتر 1 و 2 في هذه الحالة يوجد راوترين تم تفعيل بروتوكول الـ RIPv1 عليهم عندما ا يريد راوتر 1 أن يقوم بإرسال التحديثات لـ راوتر 2 سيقوم بعمل البث المباشر Broadcast 255.255.255.255 في هذه الحالة سيتم إرسال التحديثات لكل الراوترات الموجود في الشبكة بمعنى ستصل لـ راوتر 1 و 2 و 3 و 4 مع العلم انى راوتر 3 و 4 لم يتم تفعيل بروتوكول الـ RIPv1 بلا تم تفعيل بروتوكولات مختلفة مثل راوتر 3 مفعل عليه بروتوكول IS-IS و راوتر 4 مفعل عليه بروتوكول OSPF و مع هذا الاخلاف سيتم وصول التحديثات لهم و عند وصول التحديثات لهذه الراوتر سترى إنه لا تنطبق معهم ستقوم الراوترات بعملية الالغاء مما يعمل ثقل في الشبكة و سيتم فقط وصول التحديثات لـ راوتر 1 و 2 فقط التي تعمل في بروتوكولات الـ RIPv1 اما في الإصدار الثاني تم حل هذه المشكلة بعمل عنوان بث مباشر جديد يعمل فقط مع بروتوكول الـ RIPv2 تابع الشرح التالي.

- عنوان البث المباشر الذي في بروتوكول RIPv2 الإصدار الثاني 224.0.0.9

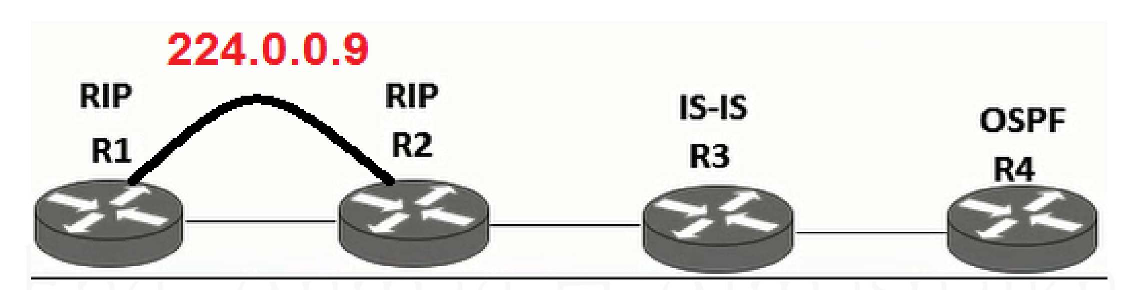
يعمل هذا العنوان على البث المباشر المخصص فقط في الراوترات التي تم تفعيل بروتوكول الـ RIPv2 فقط لا غير من دون أن تقوم بإرسال التحديثات لكل الراوترات الموجود التي

تعمل في بروتوكولات اخرى بمعنى لو كان لدينا راوترين في الشبكة **R1** و **R2** تم تفعيل بروتوكول الـ **RIPv2** فقط على هذه الراوترات فقط يريد **R1** أن يرسل تحديثات لـ **R2** سيقوم بعمل البث المباشر على العنوان التالي **224.0.0.9** وسيتم إرسال التحديثات فقط للراوترات التي تعمل ببروتوكول **RIPv2** فقط لا غير على عكس الأول .

هذا النموذج يوضح عملية البث المباشر في الإصدار الأول لبروتوكول الـ RIPv1



هذا النموذج يوضح عملية البث المباشر في الإصدار الثاني لبروتوكول الـ RIPv2



- **يعمل بخوارزمية أقصر مسار بمعنى إنه ينتمي لـ Distance Vector Protocol**
- الإصدار الأول من بروتوكول الـ **RIPv1** يعمل بنظام الـ **Classfull** بمعنى إنه لا يدعم تقسيم الشبكات مثل **VLSM** و **Subnetting** .
- الإصدار الثاني من بروتوكول الـ **RIPv2** يعمل بنظام الـ **Classless** بمعنى إنه يدعم تقسيم الشبكات مثل **VLSM** و **Subnetting** .
- **عيوب بروتوكول الـ RIP :**

عيب هذا البروتوكول إنه يقوم بعملية إرسال جدول التوجيه كل 30 ثانية في حال تم التعديل على الجدول أو لم يتم التعديل يقوم بعملية الإرسال و هذا عيب في البروتوكول لي إنه يقوم بضغط و اشغال الشبكة من غير فائدة و يحدث ثقل للشبكة لهذا السبب بروتوكول الـ **RIP** غير مستخدم كثيراً ولكن يجب أن نتعرف عليه و نفهم كيف يعمل و ما هي الخصائص التي يعمل عليه ليسهل علينا فهم البروتوكولات الآخر مثل بروتوكولات الـ **EIGRP** و **OSPF** و غيرهم من البروتوكولات .

- **تواقيت بروتوكول الـ RIP :**

١- **توقيت التحديث Update Timer** المستمر بشكل لجدول التوجيه و هذا التوقيت يستمر في الإرسال كل **30** ثانية يقوم بإرسال كامل جدول التوجيه للراوترات التي تعمل معه في بروتوكول الـ **RIP** و هذا سبب سيء في هذا البروتوكول إنه يقوم باستمرار بإرسال التحديث كل **30** ثانية .

٢- **توقيت اعتبار الشبكة غير موجودة Route Invalid Timer** بمعنى إنه تم فصل أو ايقاف الشبكة سينتظر 180 ثانية إذا لم يتم الرد عليه من قبل الشبكة الآخر سيتم الانتقال لمرحلة الغاء المسار .

٣- **توقيت إلغاء المسار Hold Down Timer** بمعنى إنه سيقوم بعملية الغاء المسار بعد أن انتظر 180 ثانية سيقوم بعملية الغاء المسار.

٤- **توقيت الإلغاء Route Flash Timer** هذا التوقيت النهائي الذي سيقوم بعملية فصل كاملة للشبكة في حالة إنه انتظر 240 ثانية ولم يتم الرد عليه سيقوم بالغاء المسار بشكل نهائي .

- **إعدادات بروتوكول توجيه المعلومات RIP Configuration** :

Router > **enable**

Router # **config t**

Router (config) # **router rip**

Router (config-router) # **version 2**

Router (config-router) # **network 200.0.0.0**

Router (config-router) # **network 100.0.0.0**

RIP Configuration

إعدادات بروتوكول الـ RIP

- **الأن سنقوم ببناء شبكة مكونة من ثلاث شبكات و راوترين و سنقوم بتفعيل بروتوكول الـ RIPv2 ليقوم بعملية الربط ما بين الشبكات الثلاث نبداء ....**
- **في البداية يجب معرفة الإعدادات التي سيتم بناء الشبكات الثلاث عليها :**

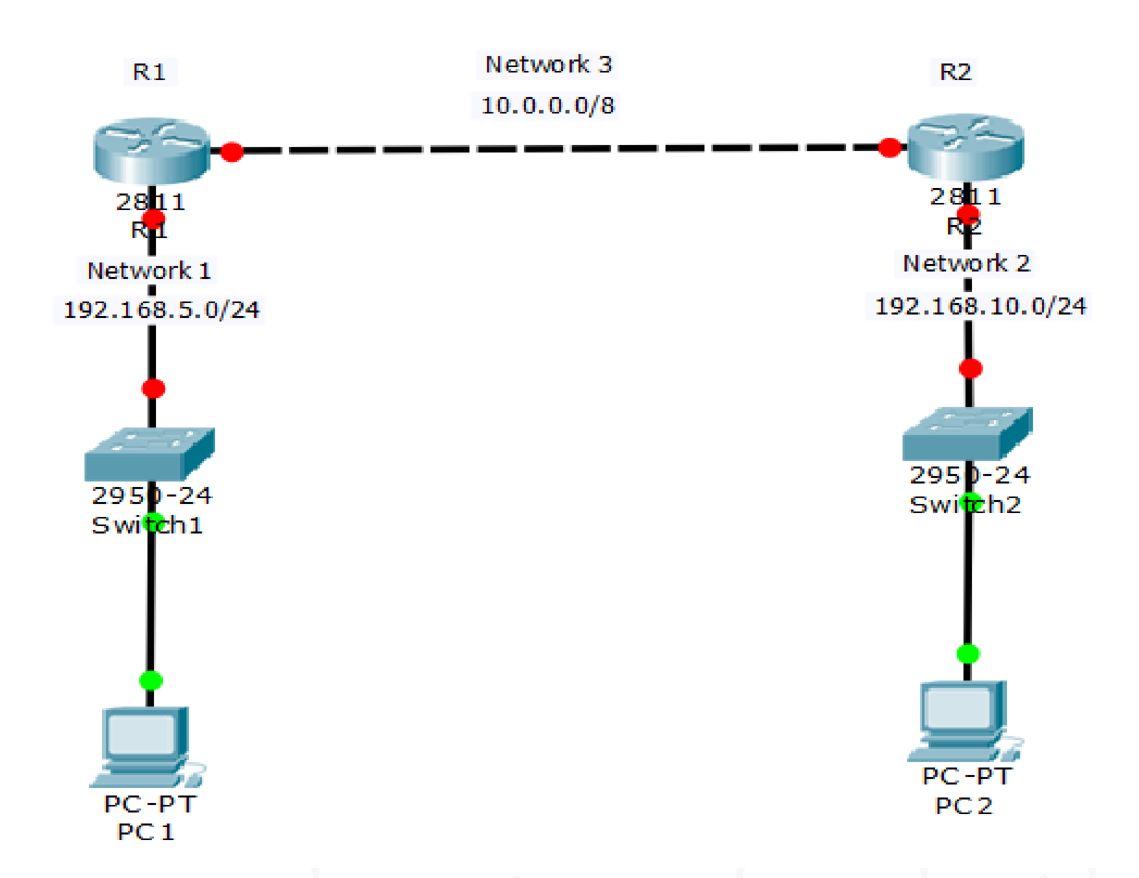
١- الشبكة الأولى ستكون بعنوان **192.168.5.0/24** .

٢- الشبكة الثانية ستكون بعنوان **192.168.10.0/24** .

٣- الشبكة الثالثة ستكون بعنوان **10.0.0.0/8** و هذه الشبكة التي ستربط ما بين الشبكة الأولى **192.168.5.0/24** و الشبكة الثانية **192.168.10.0/24** عن طريق بروتوكول الـ **RIPv2**.

٤- سنقوم بتفعيل و اعداد بروتوكول الـ **RIPv2** على **R1** و **R2** و نقوم بتعريف الشبكات في الراوترات ليتم إضافة عناوين الشبكات في جداول التوجيه ليتم الاتصال و التعرف على الشبكات بشكل صحيح .

٥- يوجد لدينا نموذج سنقوم بعمل الإعدادات عليه مكون من راوترين **R1** و **R2** و كما تعودنا سنقوم بعمل الإعدادات المعتادة سنقوم بتشغيل الإنترفيس و تركيب الاي بي لكل انترفيس و نقوم بحفظ الإعدادات و بعده نقوم بتفعيل البروتوكول و تعريف الشبكات على جدول التوجيه .



- الأن سنقوم بدخول على **R1** و عمل الإعدادات التالية :

الأن سنقوم بكتابة الاوامر التالية :

Router > **enable**

Router # **config t**

Router (config) # **interface fastethernet 0/0**

Router (config-if) # **ip address 192.168.5.1 255.255.255.0**

Router (config-if) # **no shutdown**

Router (config-if) # **exit**

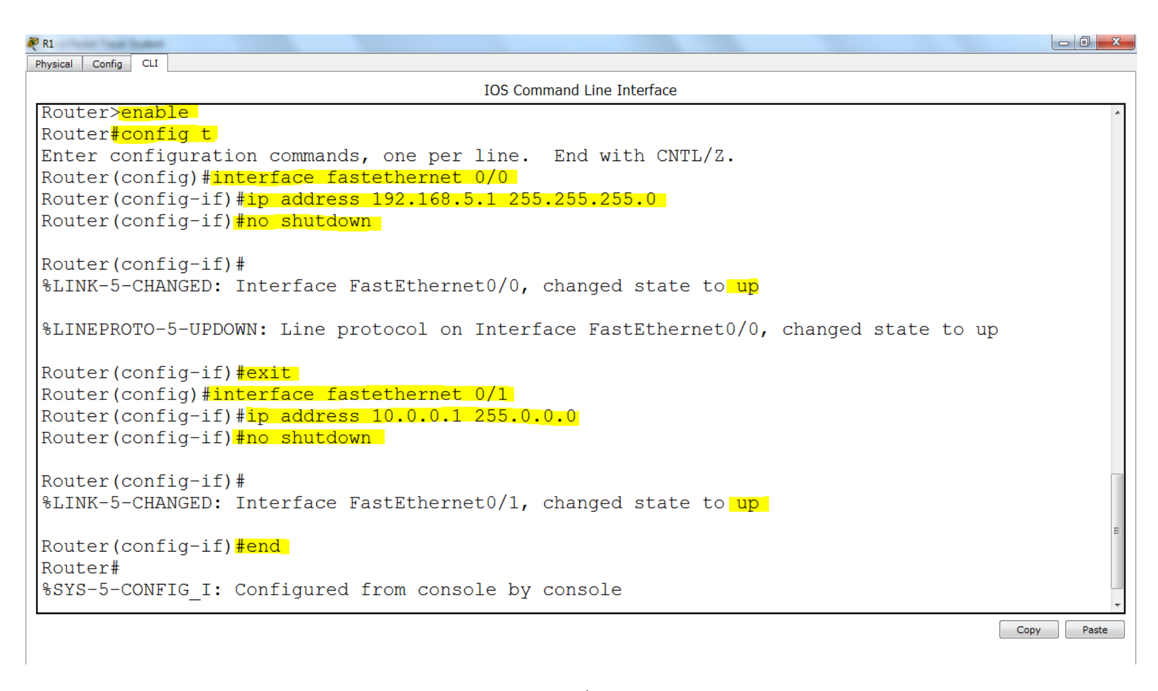
Router (config) # **interface fastethernet 0/1**

Router (config-if) # **ip address 10.0.0.1 255.0.0.0**

Router (config-if) # **no shutdown**

Router (config-if) # **end**

R1



- الأن قمنا بتشغيل الإنترفيس و قمنا ايضاً بتركيب الاي بي على انترفيس الأن سنقوم بدخول على مستوى إعدادات البروتوكولات و نقوم بتفعيل بروتوكول الـ **RIPv2** .

الأن سنقوم بكتاية الاوامر التالية :

Router # **config t**

Router (config) # **router rip**

Router (config-router) # **version 2**

Router (config-router) # **network 192.168.5.0**

Router (config-router) # **network 10.0.0.0**

```
Router#
Router#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#router rip
Router(config-router)#version 2
Router(config-router)#network 192.168.5.0
Router(config-router)#network 10.0.0.0
```

- الأن تم تفعيل بروتوكول الـ **RIPv2** على **R1** سنقوم بحفظ الإعدادات و الانتقال إلى الراوتر الآخر **R2** لنقوم بعمل نفس هذه الإعدادات عليه .

Router (config-router) # **end**

Router # **copy running-config startup-config**

- الأن سنقوم بدخول على **R2** و عمل الإعدادات التالية :

الأن سنقوم بكتابة الاوامر التالية :

Router > **enable**

Router # **config t**

Router (config) # **interface fastethernet 0/0**

Router (config-if) # **ip address 192.168.10.1 255.255.255.0**

Router (config-if) # **no shutdown**

Router (config-if) # **exit**

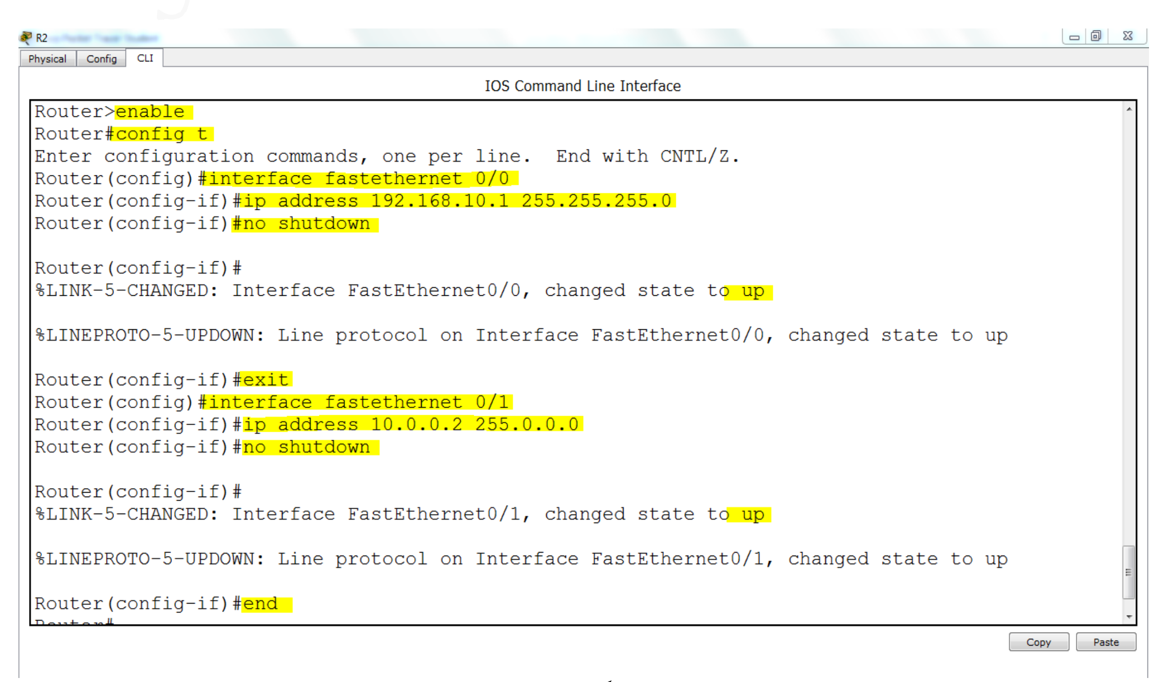
Router (config) # **interface fastethernet 0/1**

Router (config-if) # **ip address 10.0.0.2 255.0.0.0**

Router (config-if) # **no shutdown**

Router (config-if) # **end**

R2



- الأن قمنا بتشغيل الإنترفيس و قمنا ايضاً بتركيب الاي بي على انترفيس الأن سنقوم بدخول على مستوى إعدادات البروتوكولات و نقوم بتفعيل بروتوكول الـ **RIPv2**.

الأن سنقوم بكتابة الاوامر التالية :

Router # **config t**

Router (config) # **router rip**

Router (config-router) # **version 2**

Router (config-router) # **network 192.168.10.0**

Router (config-router) # **network 10.0.0.0**

```
Router#
Router#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#router rip
Router(config-router)#version 2
Router(config-router)#network 192.168.10.0
Router(config-router)#network 10.0.0.0
Router(config-router)#
```

- الأن تم تفعيل بروتوكول الـ **RIPv2** على **R2** سنقوم بحفظ الإعدادات.

Router (config-router) # **end**

Router # **copy running-config startup-config**

الأن قمنا بعملية الربط ما بين الثلاث شبكات بشكل صحيح و تم تفعيل بروتوكول الـ**RIPv2** و الأن نستطيع الاتصال في كل الشبكات الموجودة في تعمل و سنقوم بدخول على جدول التوجيه في الـ **R1** و **R2** لي نستعرض جدول التوجيه :

Router # **show ip route**

R1

```
Router#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

C    10.0.0.0/8 is directly connected, FastEthernet0/1
C    192.168.5.0/24 is directly connected, FastEthernet0/0
R    192.168.10.0/24 [120/1] via 10.0.0.2, 00:00:23, FastEthernet0/1
Router#
```

- لاحظ إنه تم إضافة شبكة **192.168.10.0/24** و يتم الوصول اليها عن طريق شبكة **10.0.0.2** و تم الربط من خلال بروتوكول الـ **RIPv2** , لاحظ إنه اخذ الرمز(**R**) .

Router # **show ip route**

R2

```
Router#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

C    10.0.0.0/8 is directly connected, FastEthernet0/1
R    192.168.5.0/24 [120/1] via 10.0.0.1, 00:00:21, FastEthernet0/1
C    192.168.10.0/24 is directly connected, FastEthernet0/0
Router#
```

- لاحظ إنه تم إضافة شبكة **192.168.5.0/24** و يتم الوصول اليها عن طريق شبكة **10.0.0.1** و تم الربط من خلال بروتوكول الـ **RIPv2** , لاحظ إنه اخذ الرمز (**R**) .

- الأن سنقوم بعملية اختبار الاتصال هل الشبكة الأولى **10.0.0.1** تستطيع الاتصال في الشبكة الثانية **10.0.0.2** سنقوم بعملية اختبار عن طريق الأمر **Ping** ما بين الـ **R1** و **R2** و سنقوم بعد هذا الاختبار سنقوم بعمل اختبار إرسال **Packet** عن طريق أجهزة الحاسوب التي متصلة في كل شبكة من الشبكة الأولى و الثانية ليتم الاختبار هل أجهزة الحاسوب تسطيع الاتصال في بعضها البعض في الشبكات المختلفة أو لا .

- سنقوم بدخول على الـ **R1** و نقوم بكتابة الأمر التالي **Router # ping 10.0.0.2** إذا تم الرد من قبل الـ **R2** بعلامة **!!!!!** فهذا يدل على إنه تم الرد بشكل صحيح اما إذا تم الرد بعلامة **.....** فهذا يدل على إنه يوجد مشكلة و لا يوجد اتصال ما بينهم .

R1

```
Router#ping 10.0.0.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.0.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/1 ms

Router#
```

- لاحظ إنه تم الرد بعلامة **!!!!!** هذا يدل على أن الاتصال صحيح و الشبكة متصلة في بعضها البعض .

R2

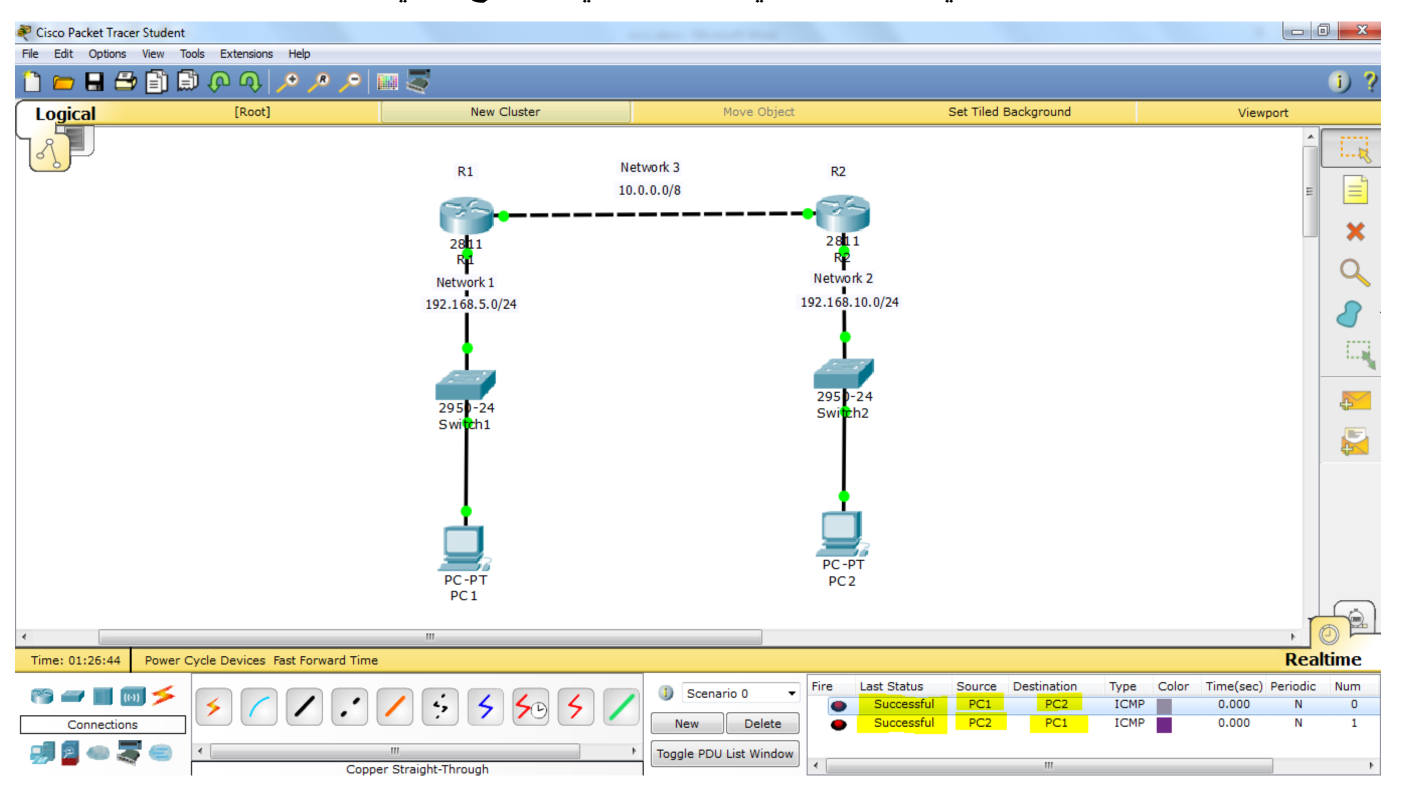
```
Router#ping 10.0.0.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.0.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/1 ms

Router#
```

- لاحظ إنه تم الرد بعلامة **!!!!!** هذا يدل على أن الاتصال صحيح و الشبكة متصلة في بعضها البعض

- الأن سنقوم بعملية الاختبار عن طريق أجهزة الحاسوب عن طريق الـ **Packet** إرسال **Packet** لجهاز معين في شبكة معينة لي نرى ذالك في النموذج التالي .

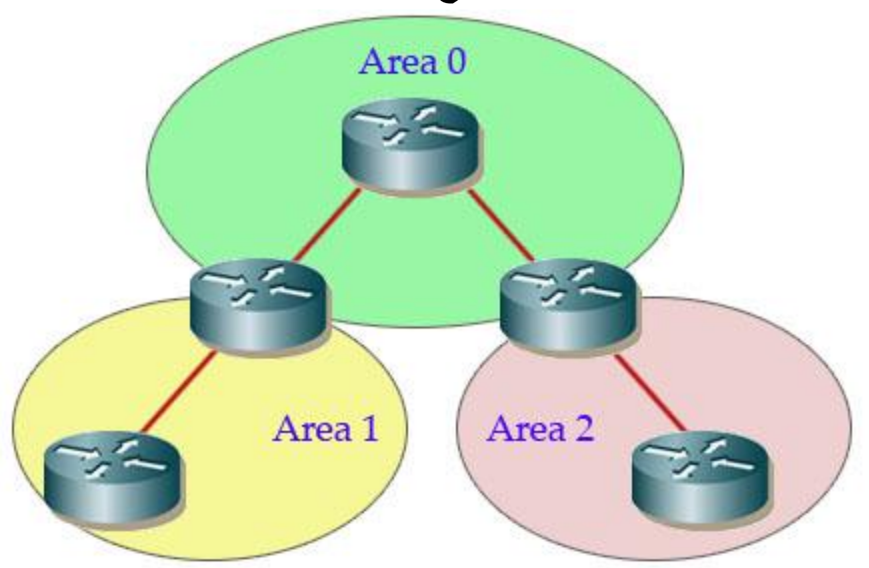


ملاحظة بسيطة : بروتوكول الـ **RIP** لا يستخدم بكثرة مثل بروتوكول الـ **EIGRP** و **OSPF** بلا هو بروتوكول صغيرة و يستخدم في الشبكة الغير كبيرة ولا الغير صغيرة بمعنى إنه يستخدم في الشبكة متوسطة الحجم مثل عندما نريد عمل شبكة مكونة من اربعة أو خمسة راوترات نقوم بعداد بروتوكول الـ **RIP** لي إنه يوفي بالغرض و لا نقوم بتفعيل البروتوكولات الضخمة مثل الـ **EIGRP** أو **OSPF** هذه البروتوكولات نحتاجه في الشبكات الكبيرة و العملاقة.

OSPF

Open shortest Path First

بروتوكول فتح أقصر مسار أولاً



فتح أقصر مسار أولا (OSPF) : هو عبارة عن بروتوكول توجيه من عائلة **link state** يستخدم مع بروتوكول الانترنت بتحديد، و يستخدم خوارزمية **Link State Routing** .

و يقع تحت مجموعة من بروتوكولات التوجيه الداخلية، التي تعمل ضمن نظام مستقل بذاته **Autonomous System** ويعرف بأنه النسخة الثانية للـ **OSPF** .

OSPF قد يكون الأكثر استعمالا في بروتوكولات البوابه الداخلية **IGP = Interior Gateway Protocol**، في مشاريع الشبكات الكبيرة .

النظام الوسيط إلى النظام الوسيط : هو أيضاً بروتوكول توجيه ديناميكي من عائلة **link state** و هو أكثر شيوعا في الخدمات الكبيرة لمزود الشبكات.

والأكثر استعمالا بروتوكول البوابه الخارجى هو بروتوكول بوابة الحدود (**BGP**) ، وبروتوكول التوجيه الرئيسي بين الأنظمة المستقلة في الإنترنت.

نظرة عامة OSPF : هو برتوكول البوابه الداخلية التي تسلك بروتوكول الإنترنت (**IP**) ويتم تجميعها فقط ضمن مجال توجيه واحدة (نظام الحكم الذاتي). إنه يقوم بجمع أنظمة المعلومات من الطرق المتاحه وبناء خريطة طوبولوجية للشبكه .

وتلك الخريطة تحدد جدول التوجيه المقدم إلى طبقة الإنترنت وهو ما يجعل توجيه القرارات تستند على الوجهة فقط ولقد اوجدت عناوين برتوكولات الانترنية .

OSPF يقوم بالكشف عن التغييرات في الطوبولوجى، كما يعمل -أيضا في حالة فشل الارتباط -، بسرعة كبيرة ويتقارب في حلقة جديده خالية من توجيه هيكل في غضون ثوان. كان يحسب أقصر طريقة لكل مسار باستخدام أسلوب مبنى على ديكسترا خوارزمية ، وهو أقصر طريق أولى للخوارزمية اعد في ربط المعلومات أي الحفاظ على كل مسار كارتباط بقاعدة بيانات (**LSDB**) التي صوره شجريه للشبكة الطوبولوجيا بأكملها. ويتم تحديث نسخة مطابقة لل **LSDB** بشكل دوري من خلال غمر جميع نطاقات **OSPF**

سياسات التوجيه الخاصه في **OSPF** لبناء جدول التوجيه تحكمها عوامل التكلفة والمقاييس الخارجية المرتبطة بكل مسارات التوجيه.

وقد تكون عوامل التكلفة المسافة من التوجيه (ذهابا وإيابا)، وإنتاجيه الشبكة للرابط أو ارتباط المتاح والدقه، كما يعرب عن أرقام بسيطه لا يمكن مقارنتها. مما يوفر وسيلة ديناميكية لتحميل متوازن للمرور بين الطرق ذوات التكلفة المتساوية.

قد يكون وجود شبكة **OSPF** ، أو تقسيمها لاى طرق، في مجالات لتبسيط التوجيه والإجراءات الإدارية وتحسين حركة المرور واستخدام الموارد. المناطق التي يتم تحديدها ب **32** جزء، تم الأعراب عنها ببساطة في العشرية، أو في كثير من الأحيان في المستند الثوماني نقطه التدوين العشري، مألوفة من **IPv4** التدوين.

من الاتفاقية ، فان المنطقة **0** (صفر) أو **0.0.0.0** تشكل جوهر أو العمود الفقري الخاص بشبكه **OSPF**

وتحديد مجالات أخرى يمكن اختيارها عن طريق الإرادة، في كثير من الأحيان ل برتوكولات الإنترنت الموجهة الرئيسية في مناطق كما في المناطق المحددة الهوية كل مجال من المجالات الإضافية يجب أن يكون لها اتصال مباشر وظاهري للعمود الفقرى الخاص بمناطق **OSPF**. مثل هذه الاتصالات هي التي تحتفظ بها جهاز توجيه مترابطة، والمعروفة باسم منطقة الراوتر الثانوية **ABR**. (**ABR**) يحافظ على ربط قواعد البيانات المنفصلة لكل منطقه من المناطق التي يتم خدمتها والمحافظه علي الطريقة الملخصه لجميع المناطق على الشبكة.

OSPF لا يستخدم بروتوكول النقل **UDP** وبرنامج التعاون الفني، ولكن يتم التغليف بشكل مباشر في مخططات برتوكولات الإنترنت مع بروتوكول رقم **89**. هذا هو على النقيض من بروتوكولات التوجيه الآخر ى، مثل بروتوكول توجيه المعلومات **RIP** ، أوبروتوكول بوابة الحدود (**BGP**) . **OSPF** تقوم بتولى اكتشاف اخطائها والعمل على تصحيحها.

معلومات قبل الدخول في تفاصيل

OSPF

- يعمل بروتوكول الـ **OSPF** في الطبقة الرابعة من طبقات الـ **OSI Layer**.
- بروتوكول بوابة داخلية **Interior Gateway Protocol** = **IGP**.

- بروتوكول عامة **Standard**.
- ينتمي لـي عائلة **Link State Protocol** .
- بروتوكول مفتوح المصدر **Open Source**.
- يعمل بخوارزمية أقصر مسار **SPF = Shortest Path First OR Dijikstra Algorithm**.
- يعمل فقط مع بروتوكول الانترنت **IP = Internet Protocol**.
- لا يعمل مع بروتوكولات **IPx** و **Apple Talk** .
- يستخدم خوارزمية **SPF** لحساب أفضل مسار .
- لا يوجد له حدود لعدد القفزات **Has Unlimited hop count** .
- تم تصميم هذا البروتوكول من قبل مهندسين الانترنت .
- قيمة المسافة الإدارية **Administrative Distance 110**.
- يدعم تقسيم عناوين الشبكات مثل **VLSM** و **Subnetting** .
- يعمل بنظام التجزئة **Classless** بمعنى تقسيم العناوين .
- إمكانية إرسال البيانات على اكثر من مسار بعدد اقصى **4** مسارات متساوية **Load Balancing to 4 equal Paths**.
- يعمل على تحديثين التحديث الفوري و التحديق الدوري **Triggerd Update and Periodic Update**.
- يحتوي على ثلاثة جداول : جدول قاعدة البيانات **(Topology Table)** و جدول الجيران **(Neighbor Table)** و جدول التوجيه **(Routing Table)** .
- يعتمد على التصميم الهرمي في عملية بناء الشبكة و هو تقسيم الراوترات على مناطق **Area**.
- النظام المعتمد عليه هذا البروتوكول هو نظام المتري وهو تكلفة المسار الاقل **Cost**. **it is the Metric** و الذي يتم حسابه من خلال سرعة المسار الافضل .
- يعتمد على إرسال رسالة تذكير أو ترحيب كل وقت معين و يستطيع مهندس الشبكة أن يقوم بضبط الوقت الخاص في رسالة الترحيب و تفيد هذه الرسالة عندما ا ترسل للراوترات الآخر أن تقوم بتاكيد على الراوترات إنهم موجودين في داخل الشبكة أو لا .
- عناوين البث المعتمد في الـ **OSPF** يوجد عنوانين بث واحد لـ **OSPF Routers** و **224.0.0.5** و واحد لـ **OSPF DR 224.0.0.6** .

OSPF Tables، جداول الـ OSPF

١- جدول الجوار Adjacency Database OR Neighbor Table

هذا الجدول المسؤولة عن الراوترات المجاورة له التي تعمل في بروتوكول الـ **OSPF** ليتم التعرف عليهم و بناء العلاقة ما بينهم و يقوم ايضاً بإرسال رسالة ترحيب ليتاكد من وجودهم في داخل الشبكة ليبقى الاتصال مفعل ما بين الراوترات الخاصة في بروتوكول الـ **OSPF** و هذا الجدول الذي يتم فيه تسجيل اسماء الرواترات المجاورة له .

الأمر الذي يقوم بعرض هذا الجدول هو الأمر التالي :

Router # show ip ospf neighbors

٢- جدول الطوبولوجي أو قاعدة البيانات Topology Table أو يطلق عليه LSDB = Link State Data Base

هذا الجدول الذي يحتوي على طوبولوجي الشبكة كلها بحيث يعرف جميع مسارات الشبكات و اسماء جميع الشبكات و الراوترات و يقوم بتخزين هذه المعلومات في داخل جدول يسمى جدول الطوبولوجي أو جدول قاعدة البيانات الذي يحتوي على جميع معلومات الشبكات , هذا الجدول يقوم بعملية التحديث مثل إضافة شبكة أو حذف شبكة أو تغير شبكة سيقوم هذا الجدول بعملية التحديث و سيقوم بإرسال التحديثات لجميع الراوترات المجاورة له ليتم التعرف على المعلومات التي تم اضافته أو حذفه لتبقى جميع الراوتر لديه نفس المعلومات و نفس قاعدة البيانات , هذا العمل يعتمد على على التحديثات التي قمنا بذكرها في بداية الـ **OSPF** و يوجد لدينا نوعان من التحديثات التحديث الدوري و التحديث الفوري هذا الجدول يستخدم التحديث الفوري لي إنه عندما يقوم بتغير أو تعديل أو إضافة أو حذف شبكة من قاعدة البيانات يجب أن باعلم الراوترات الآخر إنه تم التعديل في قاعدة البيانات في هذه الحال سيقوم باستخدم التحدث الفوري اما التحديث الدوري يستخدم بشكل منظم مثل يكون محدد له وقت معين لعملية الاستكشاف أو الكشف عن الجيران و التاكد من وجودهم في داخل الشبكة.

الأمر الذي يقوم بعرض هذا الجدول هو الأمر التالي :

Router # show ip ospf database

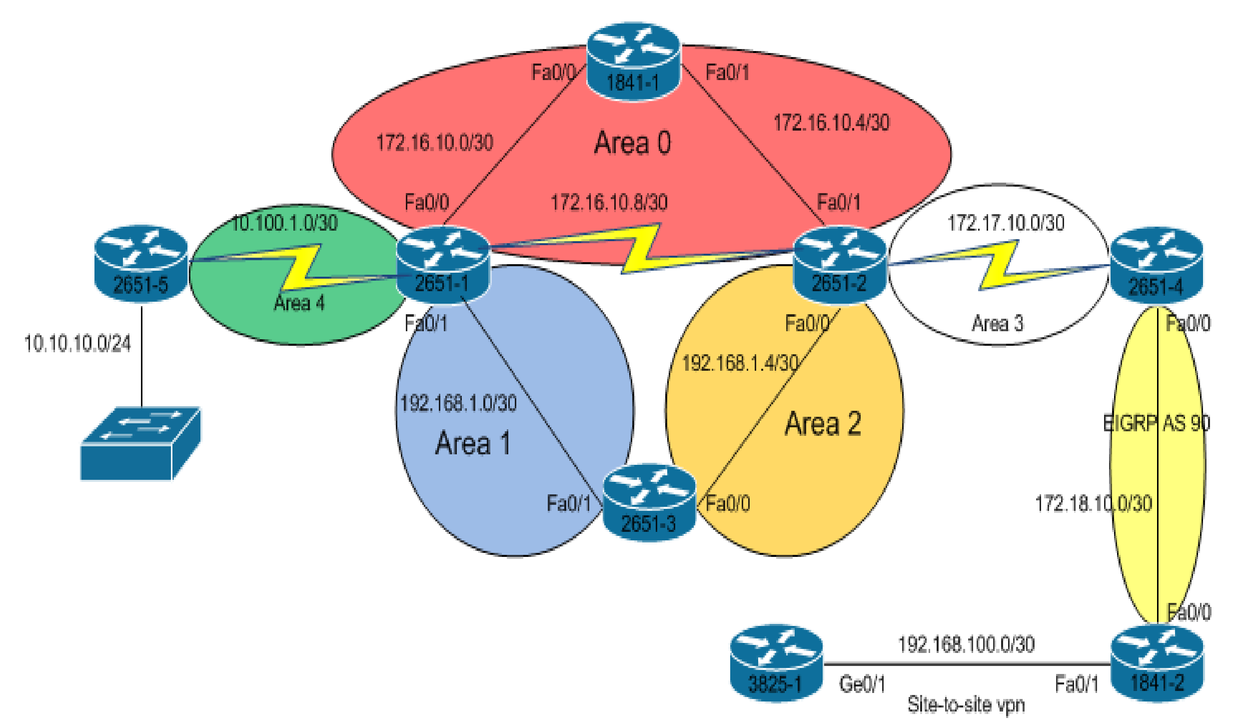
٣- جدول التوجيه Routing Table OR Forwarding Database

هذا الجدول الذي يتم فيه تسجيل جميع العناوين و جميع مسارات الشبكات و مسافة كل شبكة , حيث عندما ا يرد جهاز حاسوب في شبكة أن يتصل أو يرسل بيانات لشبكة اخرى موجودة في نطاق اخرى سيقوم جدول التوجيه في هذه المهمة حيث أن جهاز الحاسوب لا يعمل عن مسار الشبكة أو مسافة الشبكة فقط جهاز الحاسوب سيقوم بطلب إرسال سيتم الوصول لجهاز الراوتر و جهاز الراوتر سيقوم بنظر في جدول التوجيه بعده سيقوم باخذ المسار المناسب لعنوان الشبكة المطلوبة و سيتم الإرسال عليها ، هذا الجدول سيتم تبادله ما بين الراوترات

في توقيت زمني معين يقوم مهندس الشبكة بضبط إعدادات الوقت حيث يتم التبادل ما بين الراوترات هذا الجدول ليصل لكل الراوترات التي في الشبكة ليتم التعرف عليه و معرفة جميع المسارات .

الأمر الذي يقوم بعرض هذا الجدول هو الأمر التالي :

Router # show ip ospf route



مناطق بروتوكول الـ OSPF Area , OSPF

- **Area مناطق بروتوكول الـ OSPF :** هي المناطق التي يتم تقسيمها إلى عدة مناطق مثل فروع للشبكة نفسه في مناطق مختلفة عن بعضها البعض و تبداء من المنطقة **Area0**.

مثال على المناطق : يوجد لدينا شركة لديها اكثر من فرع على مختلف المدن و نريد أن نقوم بربط هذه الفروع في بعض سنقوم بعمل **Area 0** و هي التي ستقوم بربط جميع الفروع في بعضها البعض و بعد أن نقوم بعمل **Area 0** التي ستقوم بربط جميع الفروع سنقوم بتقسيم الشبكة إلى عدة مناطق مثل **Area 3** , **Area 2** , **Area 1** على مختلف المناطق و سنقوم بربطهم في الـ **Area 0** ليتمكنون من الاتصال في جميع المناطق عن طريق المنطقة الرئيسية **Area 0** .

- يوجد نوعان من تقسيم المناطق Area :

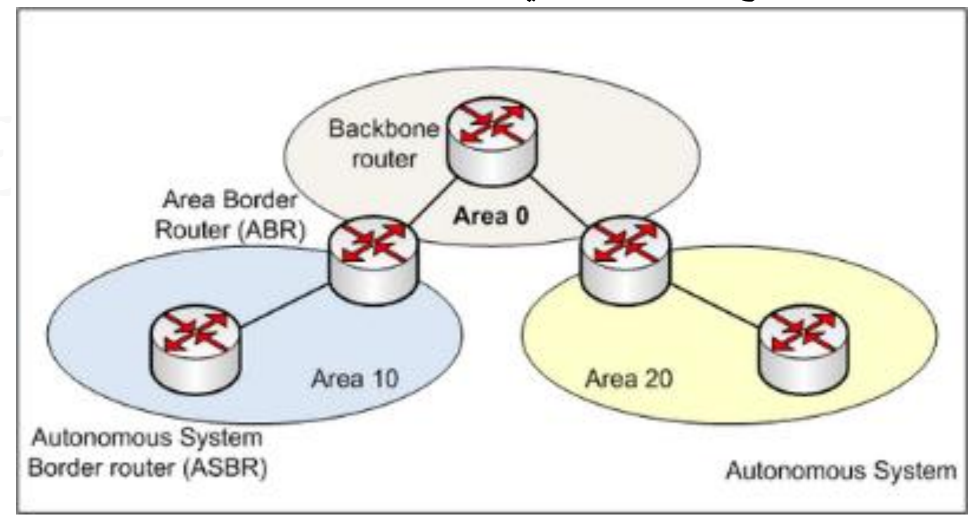
١- Backbone Area OR Transit Area

هذه المنطقة تصنف من المنطقة الرائيسية لإنه تقوم بعملية الربط ما بين مناطق مختلفة مثل **Area 2** , **Area 1** و هذه المنطقة تمسى المنطقة **Area 0** التي تربط **Area 1** , **Area 2** .

٢- Regular Area OR Non backbone Area

هذه المنقطة تصنف من المناطق التي تبداء ما بعد **Area 0** بمعنى إنه تبداء من **Area 1** و ما فوق فهذه المناطق سيتم ربطه مع **Area 0** لتتمكن من التوصيل مع بعضها البعض .

OSPF Routers
أنواع الراوترات في بروتوكول الـ OSPF



- يوجد أكثر من نوع من هذه الراوترات التي تعمل في بروتوكول الـ **OSPF** سأقوم بذكر هذه الأنواع و التعرف عليهم و معرفة كل نوع من هذه الأنواع ما هي وظيفته و متى نحتاج بناء هذا الراوتر و كيف تعمل .

- **تتكون هذه الراوترات من 5 أنواع سأقوم بذكرها مع الشرح :**

- OSPF يحدد الأنواع التالية للتوجيه:

١- Backbone Router

هذا النوع من الراوترات التي تعمل في داخل المنطقة صفر **Area 0** و اية راوترات تعمل في هذه المنطقة يطلق عليها **Backbone Router** .

٢- Internal Router

هذه الراوترات التي تشترك و تعمل في داخل منطقة مثل **Area 1** غير الـ **Backbone** **Router** و لديه عدد منافذ تعمل في هذه المنطقة **Area 1** .

٣- Area Border Router = ABR

هذه الراوترات التي تكون متصل فيها اكثر من منطقة **Area** و تمثل هذه الراوترات عبارة عن جسر يقوم بربط أكثر من منطقة **Area** مختلفات عن بعض مثل يكون لدنيا **Area 0** و نريد ربطه في **Area 100** سنقوم بعمل راوتر ما بين **Area 0** و **Area 100** ليقوم بعملية الربط و يسمى هذا الراوتر باسم **ABR** الذي يربط ما بين حدود المناطق .

٤- Autonomous System Border Router = ASBR

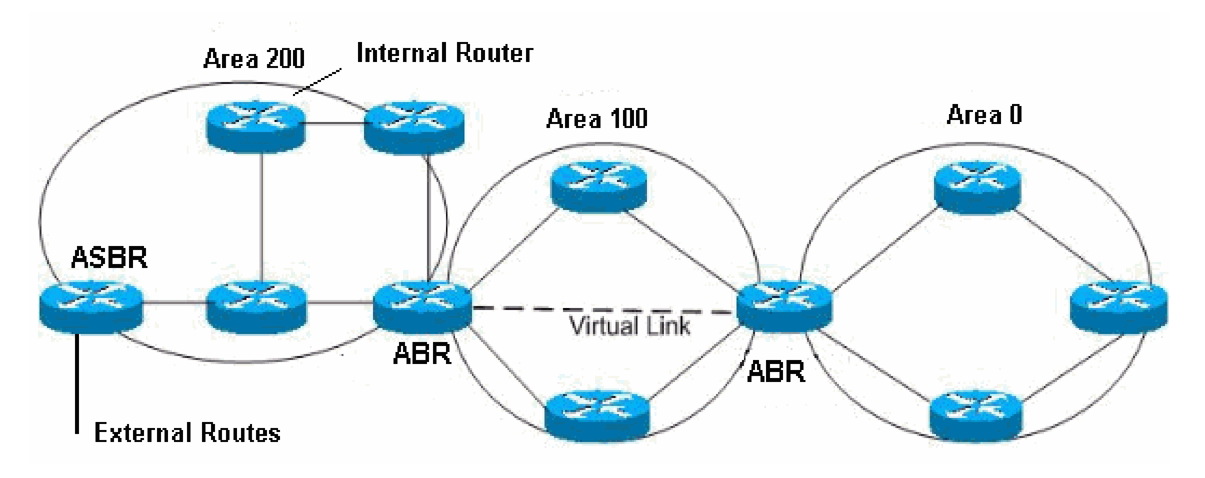
هذه الراوترات التي تقوم بربط شبكات الـ **OSPF** في شبكات مختلفة عن شبكات الـ **OSPF** بمعنى شبكة تعمل ببروتوكول مختلف عن بروتوكول الـ **OSPF** و يتم تفعيل هذه الراوتر على حدود شبكة الـ **OSPF** وليتم عمل بعض الإعدادات لتتم عملية الاتصال .

٥- Designated Router = DR

راوتر المعاينه :(DR) هو راوتر الموجهة والمختار بين كل الروترات متعلق بوصلات متعدده في قسم الشبكة ، وبصفة عامة يفترض أن يكون البث ذو وصلات متعدده. و غالبا ما تعتمد التقنيات الخاصة على وجود مورد، قد تكون هناك احتياج لدعم وظيفة التي يقوم بها **(DR)** على وصلات المتعددة بدون بث **(NBMA)** وسائل الاعلام. عادة ما يكون من الحكمة أن تكوين الدوائر الفردية الظاهري فرعية **NBMA** كمركز فردى من نقطة إلى نقطة ؛ التقنيات المستخدمة هي التي تعتمد على التنفيذ.

٦- Backup Designated Router = BDR

راوتر المعاينه الاحتياطى : (BDR) هو الراوتر الاحتياطى الذي ياخذ محل الراوتر الرئيسي في حال وقوع راوتر الـ (**DR**) سيقوم باخذ مكانه حتى يتم ارجع تفعيل الراوتر الرئيسي (**DR**) .



OSPF Networks Types

أنواع الشبكات في بروتوكول الـ OSPF

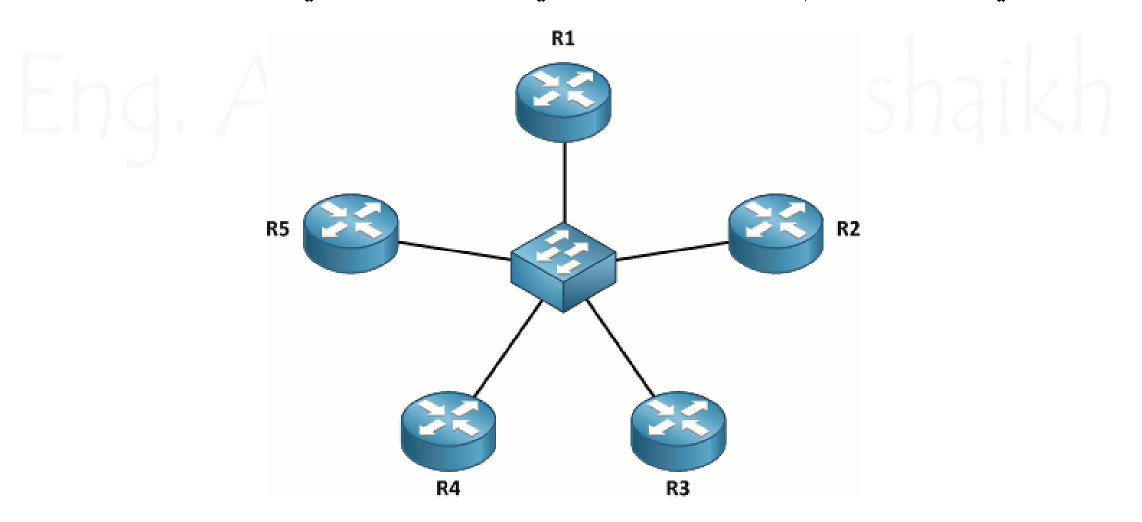
١- Point – to –Point Network

هذه الشبكة التي يتصل في راوترين ببعض وجه لوجه عن طريق بروتوكول الـ **OSPF** بشكل مباشر .



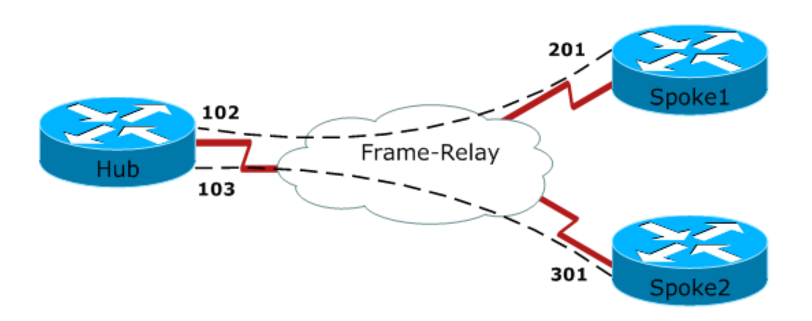
٢- BMA = Boradcast Maulti-access Network

هذه الشبكة التي تربط الراوترات من خلال السويتش في شبكة واحدة و هذه الشبكة السريعة طبعاً و في هذه الشبكة يتم اختيار راوتر رئيسي و راوتر احتياطي **DR** و **DBR** .



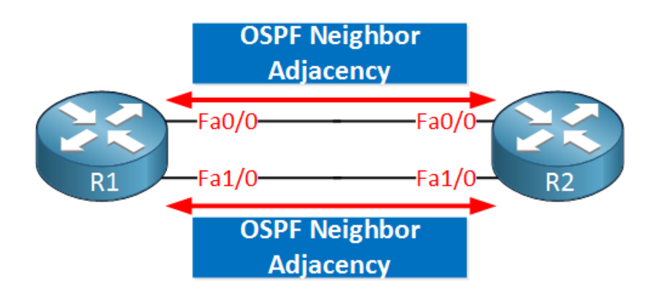
٣- NBMA = No Boradcast Maulti-access Network

هذه شبكة الوصول المتعدد بمعنى لا يوجد بث مباشر هذا الشبكة تعمل في تقنية مثل الـ **Frame Relay** أو **MPLS** .



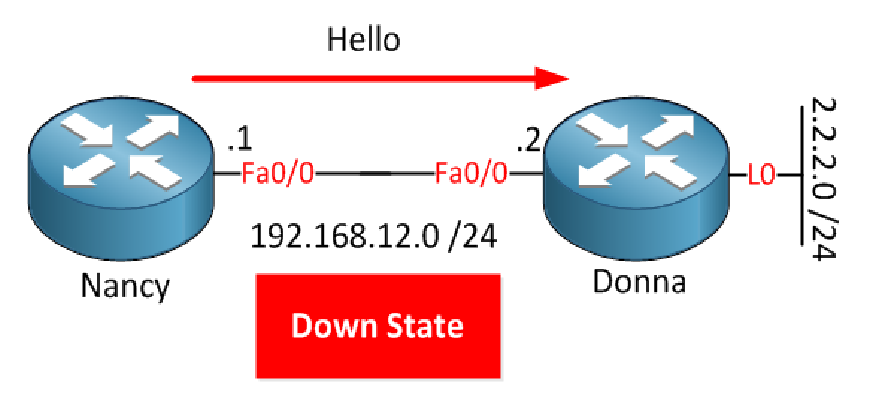
OSPF Neighbor Adjacencies

بناء العلاقات ما بين الجيران في بروتوكول الـ OSPF

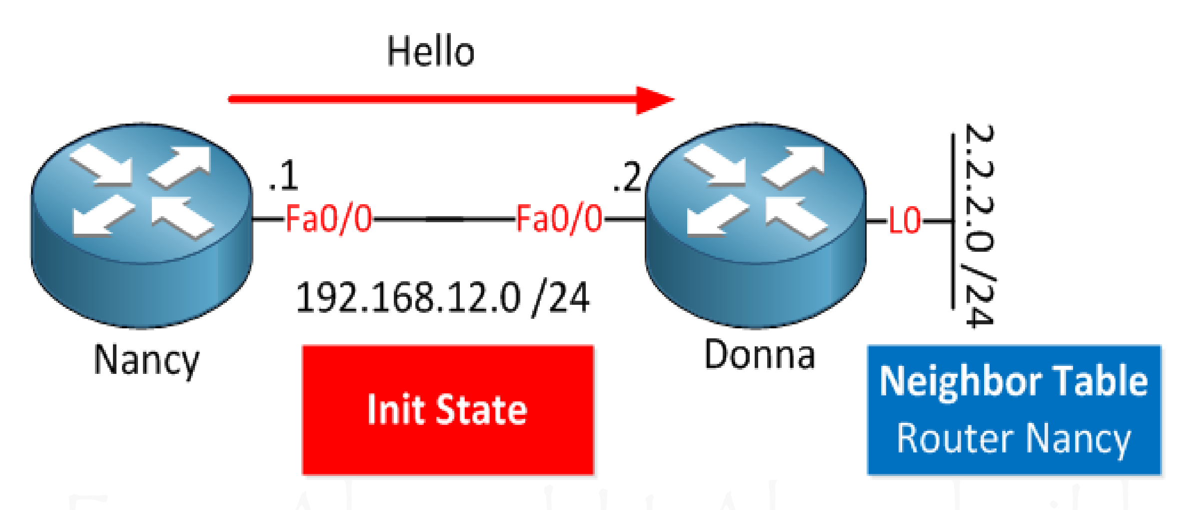


- إقامة العلاقات ما بين الجيران بمعنى الراوترات التي تعمل في بروتوكول الـ **OSPF** نريد أن تتصل في بعضها البعض و تقوم ببناء العلاقة ما بينهم و أن تقوم بتادل المعلومات و التحديثات و المسارات ما بينا جميع الراوتر لتعمل كلها في بنفس المعلومات و التحديثات و المسارات و تستطيع الاتصال في جميع الشبكات و التعرف على التغيرات و التحديثات التي تم اضافته أو حذفه أو التعديل عليها يجب تبادل جميع هذه البيانات على جميع الراوترات التي تعمل في بروتوكول الـ **OSPF** في داخل الشبكة و يحدث التبادل عن طريق **5** خطوات سأقوم بذكرها و شرح كل واحدة لوحده لنتمكن من التركيز و فهم كل واحدة على ماذا تحتوي .

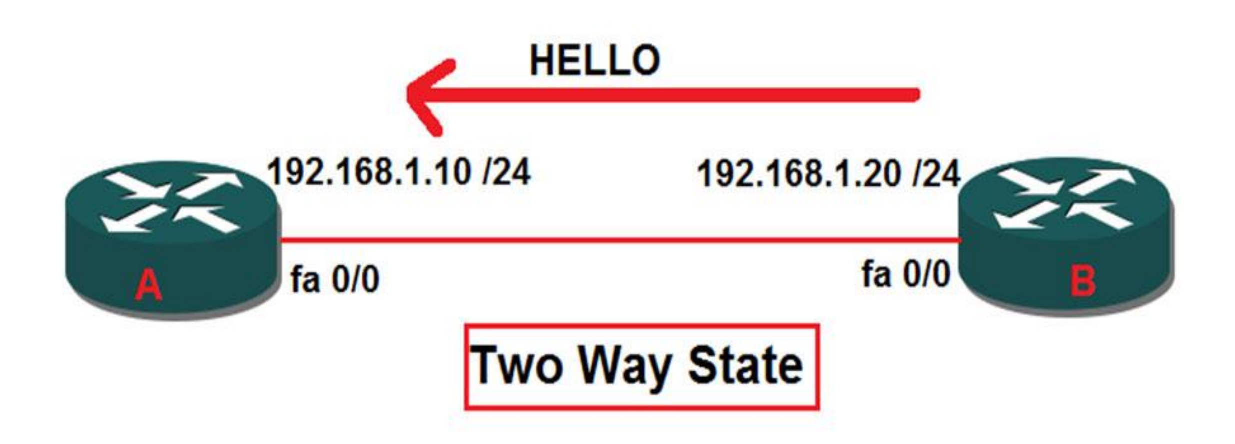
١- **Down State :** هذا حالة الراوتر عند تشغيله لي أول مره في الشبكة و قبل أن يتم تفعيل بروتوكول الـ **OSPF** في هذه الحالة يجب أن نعرف إنه لا يوجد عملية تبادل المعلومات أو ما شابه ما بين الراوترات حتى ولو كانت تم توصيلهم على سوتيش واحد فهو لا يوجد ربط ما بينا هذه الراوترات ولكن عندما ا نقوم بتفعيل بروتوكول الـ **OSPF** على أحد الراوترات أو الراوتر الرئيسي سيقوم بعملية إرسال رسالة ترحيب **Hello Packets** يستكشف فيها الجيران الموجودين معها على الشبكة و سيتم إرسال رسالة الترحيب **Hello Packets** على العنوان **224.0.0.5** بمعنى **Multicast** في الشبكات الوجه لوجه **Point – to – Point** و **Broadcast** في الشبكات السريعة التي تكون متصلة على سوتيش واحد بنفس النطاق و بنفس الشبكة ولكن في الشبكات الآخر مثل الشبكات التي يتم ربطه عن طريق الـ **Frame Relay** ستتم عملية الإرسال بشكل **Unicast**.



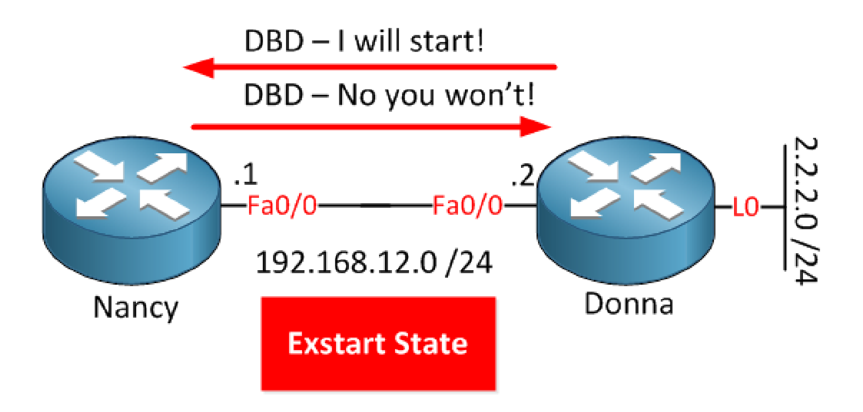
٢- **Init State:** هذه تعني أن يقوم الراوتر الرئيسي الذي تم تفعيل بروتوكول الـ **OSPF** عليه أن يقوم بعملية إرسال رسالة الترحيب **Hello Packets** لجميع الراوترات التي تم تفعيل بروتوكول الـ **OSPF** عليها في هذه الحالة سيكتشف إنه يوجد جيران له مفعل عليهم بروتوكول الـ **OSPF** سيقوم بتعديل في جدول الجيران و يقوم بتسجيل المعلومات و التحديثات و المسارات و سيقوم بتعريف عن نفسه للراوترات الآخر كل هذه المعلومات تندرج تحت جدول الجيران **Adjacency Database OR Neighbor Table.**



٣- **Two Way State:** في هذه المرحلة تقوم راوترات الجيران المتصلة في الراوتر الرئيسي والتي استقبلت رسالة ترحيب **Hello Packet** من الراوتر الرئيسي سيقوم الراوتر الرئيسي برد رسالة **Unicast Reply** يتضمن قائمة الـ **Router ID** لجميع الراوترات المتصلة بهم و معهم الراوتر الرئيسي و عند استقبال الراوتر الرئيسي لهذه الرسالة سيقوم بإضافة و تعديل الجيران في جدول العلاقات و هو **Adjacency Database OR Neighbor Table** و في هذه الحالة تسمى هذه العملية **Two Way State.**



٤- **Exstart State:** هذه الحالة عبارة عن ملخص رؤس أقلام لقاعدة البيانات **DataBase Description** أو كما تعرف **DBD** الخاصة بالمسارات الموجودة في الشبكة و ظيفة هذه العملية إنه تقوم بتاكد من كل الراوتر المجاور هل توجد نفس البيانات و قاعدة البيانات في جميع الراوترات المجاورة أو لا.



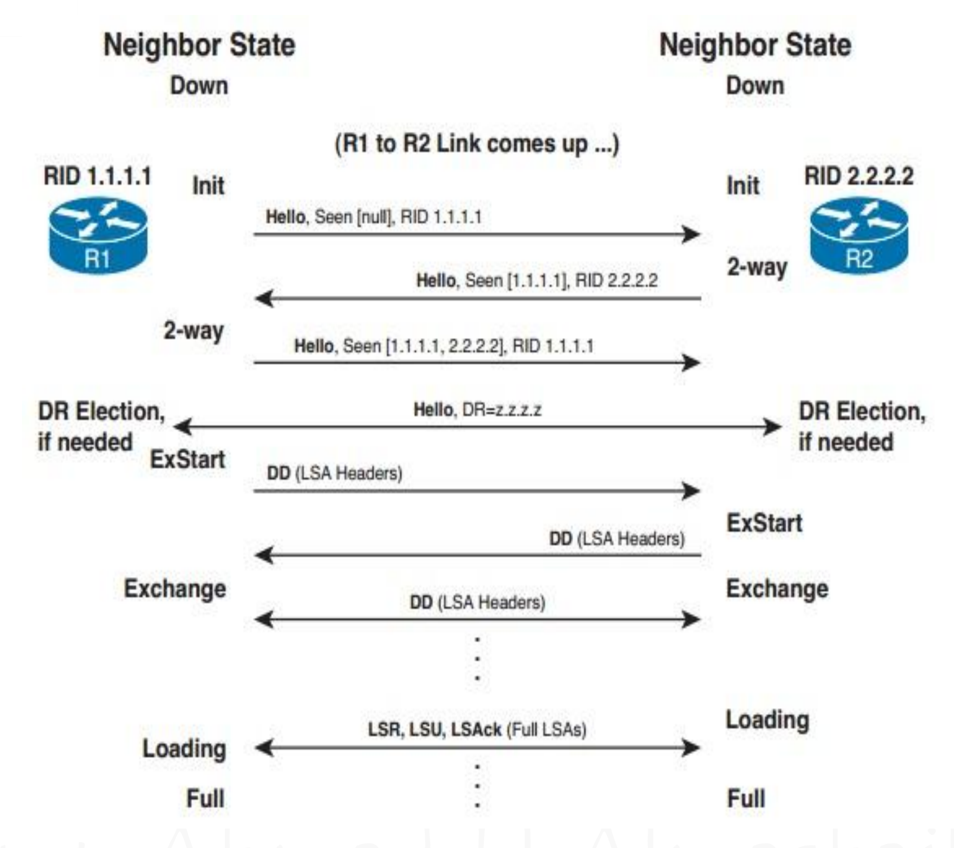
٥- **Exchange State :** هذه العملية وظيفتها تاتي بعد تحديد الراوتر الذي سيقوم بإرسال جدول قواعد البيانات **DBD** أولاً سيقوم الراوتر الذي لديه اعلى **Router ID** هو من سيقوم بعملية إرسال ملخصات **Summary DBD** وليتم معرفة ما هي قواعد البيانات التي عند الراوترات الآخر و في هذه الحالة عليه أن يعرف هل قاعدة البيانات تم تحديثها أو لا في حال إنه يوجد بعض المعلومات المتطابقة و لكي يعرف هل هذه المعلومات قديمة أو حديثة هذه من وظيفة الـ **Sequence numbers** في هذه الحالة يوجد ثلاث خطوات يجب أن يتم تبادلها من قبل الراوترات التي استقبلة **DBD** .

١- يجب على راوتر الجار أن يرد علينا إنه تم استلام **DBD** عن طريق إرسال **Link-State Acknowledgment** أو الاختصار **LSAck**.

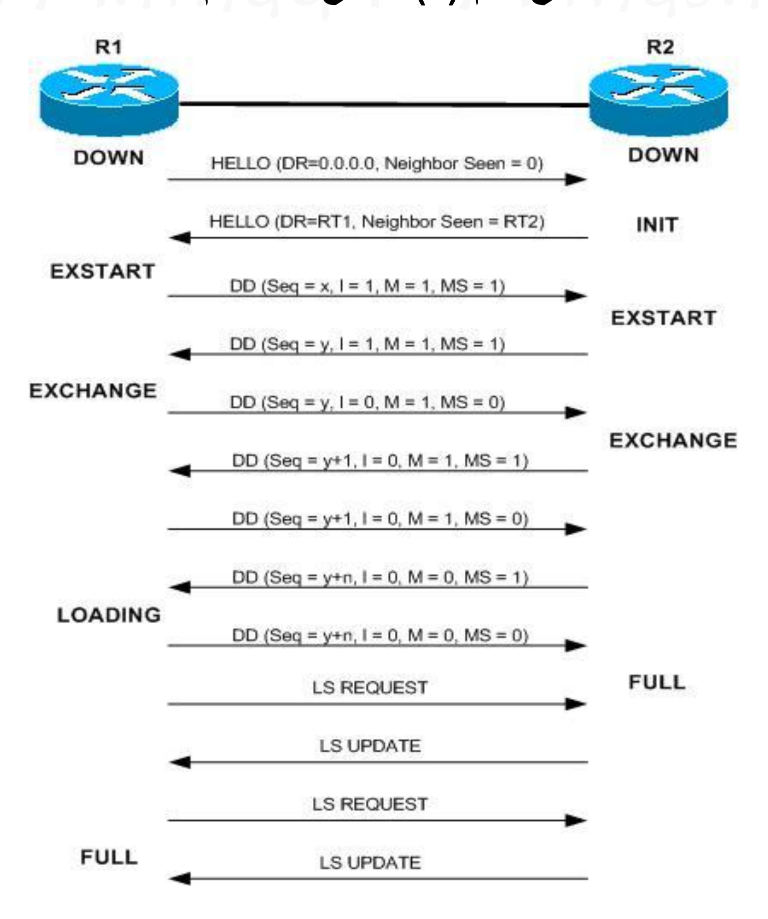
٢- يقوم الـ **Router** بمقارنة المعلومات التي استقبلها من جاره بالمعلومات التي لديه ليتأكد بأنها معلومات حديثة عن الشبكة .. وإذا كانت معلومات جاره ليست موجودة لديه أو أنها أحدث أو كما يطلق عليها **up-to-date** من التي لديه .. يقوم بإرسال **Link-State Request** أو **LSR** متضمنة المعلومة المطلوبة .. و هذه العملية عملية إرسال الـ **LSR** يطلق عليها **Loading State** .

٣- يقوم الجار بالاستجابة لهذا الطلب بإرسال تحديثات كاملة عن المعلومة المطلوبة بإرسال **Link-State Update** أو **LSU** متضمنة آخر التحديثات .. عند استقبال الـRouter الآخر لهذه التحديثات يقوم بالرد عليها بإرسال **LSAck** للجار بعد هذه المراحل و عمليات التبادل والطلب والإرسال .. تكون الراوترات في حالة تزامن لهم نفس قاعدة البيانات لـ **area** معينة .. و عند هذه النقطة تعتبر جميع الـ **Routers** في الـ **Full-State** .

هذا نموذج رقم (1) يوضح كل ما تم شرحه



هذا نموذج رقم (2) يوضح كل ما تم شرحه

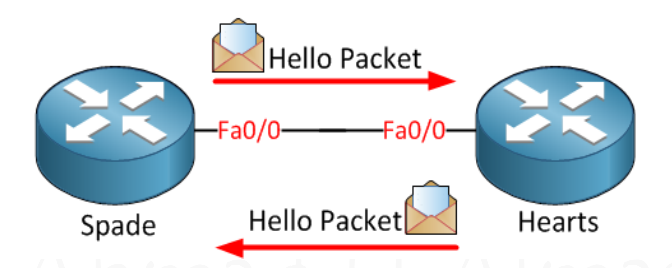


أنواع حزم البيانات الخاصة في بروتوكول التوجيه الـ OSPF

OSPF Packet Types

- حزم البيانات يتم استخدمها فيما بين الراوترات التي تم تفعيل بروتوكول الـ **OSPF** عليها لتتمكن من بناء و صيانة الجداول الثلاثة الموجودة في كل راوتر .
- تتكون حزم البيانات من **5** أنواع سأقوم بذكرها و شرح كل واحدة بشكل منفصل عن الآخر .
- قبل البداء في التعمق يجب أن نعرف أن كل **LSA** تأخذ رقم متسلسل يبداء من **0x80000001** إلى **0x7FFFFFFF** هذه الارقام مخصص للـ **LSA** .

١- **Hello Packets :** هي عبارة عن رسالة ترحيب يتم استخدامها في عملية اكتشاف الجيران و بناء العلاقة ما بينهم و بعد أن يتم اكتشاف الجيران و التعرف عليهم سيتم معاودت إرسال رسالة لتاكد من وجود الراوترات في داخل الشبكة.



- محتويات رسالة الترحيب **Hello Packets :**

1- Router ID
2- Router Priority
3- Hello (default 10s for broadcast network, default 30s for non-broadcast network) and dead (4 times of hello) timers.
4- Authentication password.
5- Area ID
6- Subnet Mask
7- Designated router and backup designated router is ip address
8- Known neighbours

هذه جميع المعلومات التي تكون في داخل رسالة الترحيب الـ Hello Packets سأقوم بشرح كل واحدة بالتفصيل .

١- **Router ID :** هو عبارة عن عنوان الاي بي الذي ياخذه أول راوتر في شبكة بروتوكول الـ **OSPF** و يجيب المعرفة أن هذه الشبكة ستكون من نوع **BMA** .

- لعرض تفاصيل الـ **Router ID** نقوم بكتابة الأمر التالي و سيقوم بعرض معلومات و تفاصيل بخصوص جدول **Neighbor Adjacency Database** .

Router # **show ip ospf interface**

بعد كتابة الأمر سيتم عرض المعلومات الخاصة في **Router ID** كما في الصورة التالية ....

show ip ospf interface

```
Router# show ip ospf interface
Ethernet0 is up, line protocol is up
  Internet Address 206.202.2.1/24, Area 1
  Process ID 1, Router ID 1.2.202.206, Network Type BROADCAST, Cost: 10
  Transmit Delay is 1 sec, State BDR, Priority 1
  Designated Router (ID) 2.2.202.206, Interface address 206.202.2.2
  Backup Designated router (ID) 1.2.202.206, Interface address 206.202.2.1
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:00
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 2.2.202.206  (Designated Router)
  Suppress hello for 0 neighbor(s)
Serial0 is up, line protocol is up
  Internet Address 206.202.1.2/24, Area 1
  Process ID 1, Router ID 1.2.202.206, Network Type POINT_TO_POINT, Cost:
   64
  Transmit Delay is 1 sec, State POINT_TO_POINT,
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:04
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 2.0.202.206
  Suppress hello for 0 neighbor(s)
```

Router ID #

Neighbor adjacencies

Timer intervals

٢- **Router Priority** : هي قيمة موجودة في جميع الراوترات التي تم تفعيل بروتوكول الـ **OSPF** عليها و هي تاتي في جميع الراوترات القيمة **Priority Default (1)**.

لعرض التفاصيل نقوم بكتابة الأمر التالي :

Router # **show ip ospf neighbor**

```
RouterA#show ip ospf neighbor

Neighbor ID     Pri  State       Dead Time   Address       Interface
192.168.31.33     1  FULL/DR     00:00:39    192.168.1.3   FastEthernet0/0
192.168.31.22     1  FULL/BDR    00:00:36    192.168.1.2   FastEthernet0/0
```

```
RouterB#show ip ospf neighbor

Neighbor ID     Pri  State          Dead Time   Address       Interface
192.168.31.33     1  FULL/DR        00:00:34    192.168.1.3   FastEthernet0/0
192.168.31.11     1  FULL/DROTHER   00:00:38    192.168.1.1   FastEthernet0/0
```

```
RouterC#show ip ospf neighbor

Neighbor ID     Pri  State          Dead Time   Address       Interface
192.168.31.22     1  FULL/BDR       00:00:35    192.168.1.2   FastEthernet0
192.168.31.11     1  FULL/DROTHER   00:00:32    192.168.1.1   FastEthernet0
```

Priority is equal at the default value of 1.

٣- Hello (default 10s for broadcast network, default 30s for non-broadcast network) and dead (4 times of hello) timers.

تواقيت رسالة الترحيب في الشبكات يوجد اكثر من توقيت لعملية إرسال رسالة الترحيب على مختلف أنواع الشبكات في الشبكات السريع تختلف السرعة و في الشبكة البطيئة تختلف السرعة و في الشبكات البعيدة تختلف ايضاً .

١- الشبكات السريعة تكون فيها عملية إرسال رسالة الترحيب كل عشر ثواني بشكل طبيعي **default 10s for broadcast network** طبعاً هذه الشبكة تكون في نفس نطاق العناوين أو تكون مرتبطة على جهاز سوتيش .

٢- الشبكات البعيدة أو البطيئة التي تكون متصلة عن طريق بروتوكول الـ **PPP** أو **MPLS** أو **Frame Relay** تكون في هذه الحالة عملية إرسال رسالة الترحيب كل ثلاثين ثانية بشكل الطبيعي **default 30s for non-broadcast network** هذه الشبكات لا تكون في نفس النطاق .

٣- و في حال لم يتم الرد أو إرسال رسالة ترحيب في غضون **40** ثانية مقسمة على اربعة رسالة **4 itmes of hello** و في كل رسالة من الاربعة رسالة يكون التوقيت **10** ثواني و يتم جمعها على اربعة رسالة و تصبح **4** رسال ترحيب و في هذه الحالة سيعتبر أن الراوتر غير موجود في الشبكة .

ملاحظة : نستطيع التعديل في التوقيت ولكن في المستوى المتقدم من هذه الدروس بمعني مستوى المحترفين .

نستطيع عرض و معرفة معلومات التوقيت الخاص في رسالة الترحيب من خلال الأمر التالي :

Router # **show ip ospf interface**

```
  Internet Address 10.0.67.7/24, Area 0
  Process ID 1, Router ID 7.7.7.7, Network Type BROADCAST, Cost: 1
  Enabled by interface config, including secondary ip addresses
  Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 7.7.7.7, Interface address 10.0.67.7
  Backup Designated router (ID) 10.0.68.6, Interface address 10.0.67.6
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    oob-resync timeout 40
    Hello due in 00:00:07
  Supports Link-local Signaling (LLS)
  Index 2/2, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 0, maximum is 4
  Last flood scan time is 0 msec, maximum is 4 msec
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 10.0.68.6  (Backup Designated Router)
  Suppress hello for 0 neighbor(s)
FastEthernet0/1 is up, line protocol is up
  Internet Address 10.0.17.7/24, Area 0
  Process ID 1, Router ID 7.7.7.7, Network Type BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 7.7.7.7, Interface address 10.0.17.7
  Backup Designated router (ID) 10.100.1.1, Interface address 10.0.17.1
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    oob-resync timeout 40
    Hello due in 00:00:08
  Supports Link-local Signaling (LLS)
  Index 1/1, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 2
  Last flood scan time is 0 msec, maximum is 4 msec
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 10.100.1.1  (Backup Designated Router)
  Suppress hello for 0 neighbor(s)
R7#
```

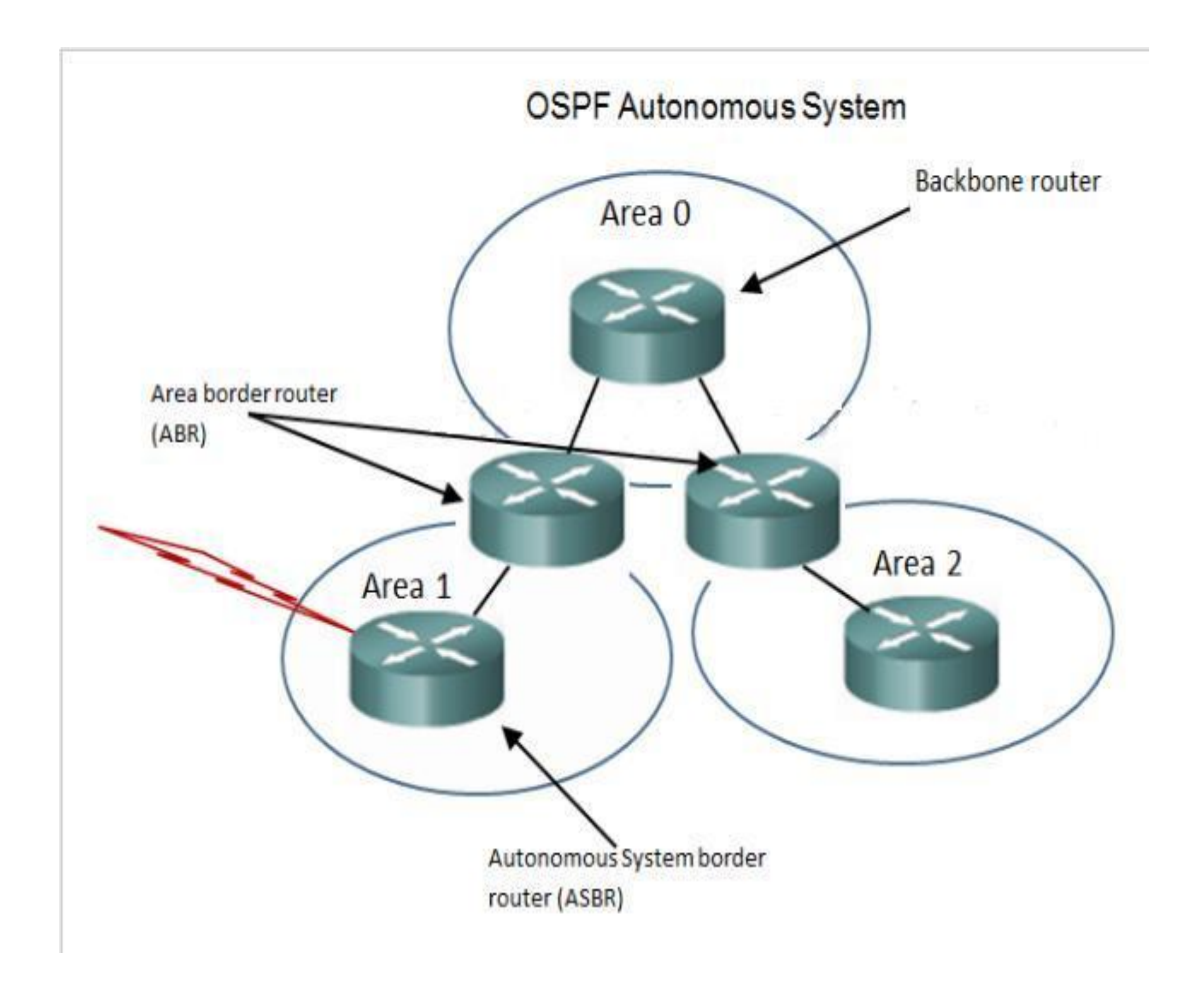
٤- **Authentication password :** هذه العملية تختص في توثيق كلمات المرور بحيث يتم تطبيق كلمات المرور على الراوترات و تتم عملية التوثيق ما بينهم لتكون في أمن.

ولعرض هذه المعلومات و التاكد من تفعيل هذه العملية نقوم بكتابة الأمر التالي :

Router # **show ip ospf interface**

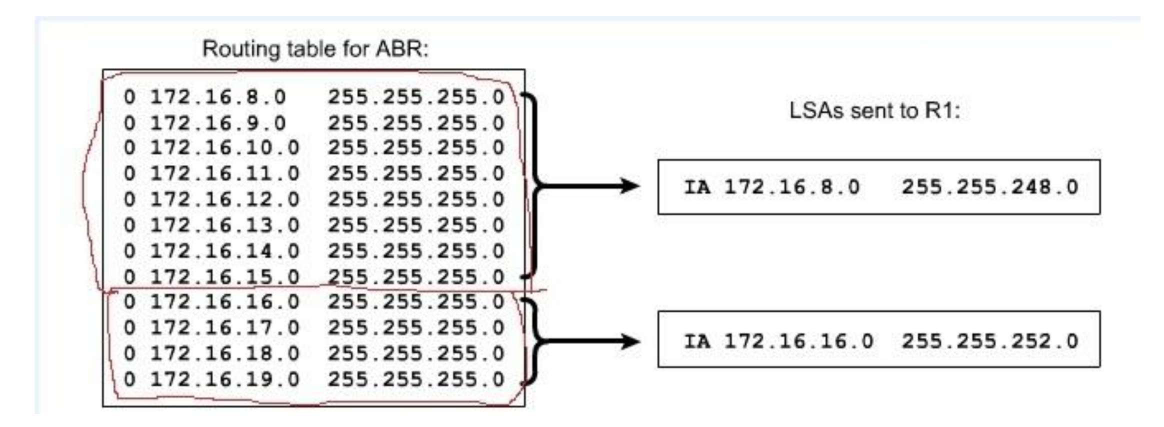
```
PA-EDGE-01-0> show ip ospf interface
vNic_1 is activated
  Internet Address 192.168.100.1, Network Mask 255.255.255.0, Area 0.0.0.10
  Transmit Delay is 1 sec, Network Type BROADCAST, State BDR, Priority 128
  Designated Router's Interface Address 192.168.100.3
  Backup Designated Router's Interface Address 192.168.100.1
  Timer intervals configured, Hello 1, Dead 3, Retransmit 5
  Simple password authentication enabled
PA-EDGE-01-0>
```

٥- **Area ID :** رقم المنطقة التي متوصل فيها مثل منطقة رقم صفر تمسى **Area 0** و التي عن طريق هذه المنطقة يتم التوصيل بمنطقة اخرى مثل **Area 100** أو غيرها .



٦- **Subnet Mask :** قناع الشبكة يجب أن يكون في داخل رسالة الترحيب ليتمكن من معرفة كل عناوين الشبكات المرسالة اليها رسالة الترحيب.

ملاحظة : قناع الشبكة لا يكتب كما نعرفه بلا يكتب بشكل معكوس في بروتوكول الـ **OSPF** بمعنى **Wildcard Mask** و سنقوم بشرح ما معنى **Wildcard Mask** في ما بعد .

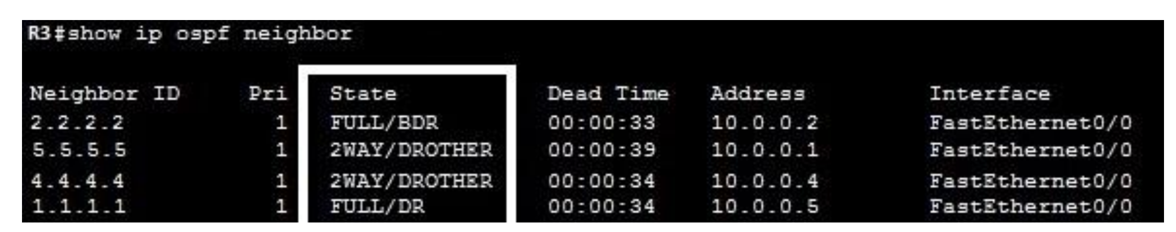


Designated router and backup designated router is ip address :

٧- في هذه العملية تكون على معرفة كاملة من هو الراوتر الرئيسي و الراوتر الاحتياطي و تحتوي على عناوين كل راوتر من هذه الراوترات **BDR** and **DR** ليتم إرسال و استقبال رسالة الترحيب بشكل صحيح.

و لعرض و معرفة حالة الراوترات و معرفة معلومات عنهم سنقوم بكتابة الأمر التالي.........

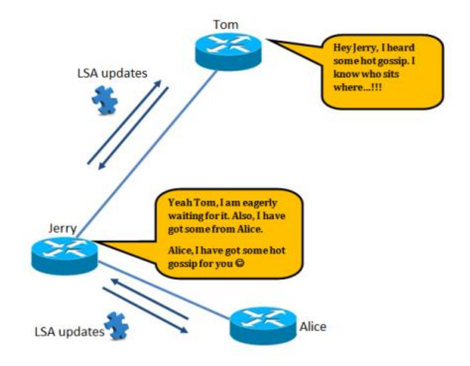
Router # **show ip ospf neighbor**



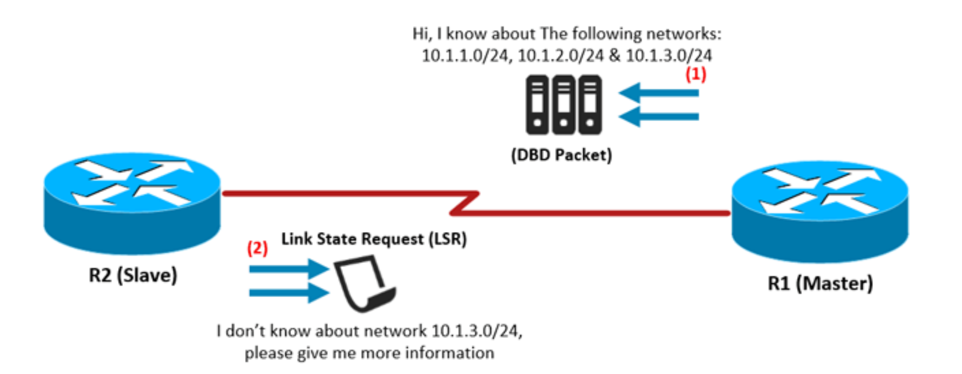
R3#show ip ospf neighbor

Neighbor ID	Pri	State	Dead Time	Address	Interface
2.2.2.2	1	FULL/BDR	00:00:33	10.0.0.2	FastEthernet0/0
5.5.5.5	1	2WAY/DROTHER	00:00:39	10.0.0.1	FastEthernet0/0
4.4.4.4	1	2WAY/DROTHER	00:00:34	10.0.0.4	FastEthernet0/0
1.1.1.1	1	FULL/DR	00:00:34	10.0.0.5	FastEthernet0/0

8- **Known neighbours :** الراوترات المعروفة في الشبكة ، حيث تقوم هذه العملية بمعرفة جميع الراوترات المجاورة في الشبكة لتسطيع التعرف على بعضها البعض و تتبادل المعلومات و البيانات .



٢- **DBD = Data Base Description :** هذه الـ **Packets** يتم تبدله ما بين الراوترات حيث يقوم كل راوتر من الراوترات بإرسال الطوبولوجي التي يحتوي عليه سيقوم بإرساله للراوترات الموجودة على الشبكة و المفعل عليه بروتوكول الـ **OSPF** و بعد وصول هذه الرسالة **Packets** لكل الراوترات ستقوم كل راوترات بعملية تحديثلقاعدة البيانات ليتم إضافة أو ازالة الشبكات أو المعلومات التي تحتوي عليها هذه الرسالة و طبعاً هذه الـ **Packet** تحتوي على عدة محتويات سأقوم بذكرها و شرحها بالتفصيل.



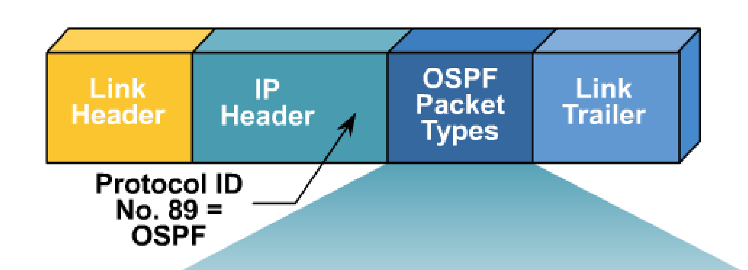
محتويات رسالة قاعدة البيانات DBD: في البداية هذه الرسالة تتكون من **Header** حجم هذا الـ **Header 31 Bit** يتكون من عدة خانة يتم تركيبها بشكل منظم و بعدا أن يتم تجميع هذه الـ **Header** سيقوم ايضاً بعمل إضافة لي رسالة الترحيب **Hello Packets** الذي شرحته من قبل .

- الأن سأقوم بذكر محتويات الـ **OSPF Packet Header** الذي تكون في داخل رسالة الـ **DBD :**

1-Version , 2- Type, 3-Packet Length , 4- Router ID , 5- Area ID,

6- Checksum, 7-AuType, 8-Authentication, 9- Data

كما في النموذج التالي



- **الأن سأقوم بشرح كل واحدة من هذه المكونات بشكل منفرد عن الآخر لنفهم وظيفة كل واحدة من هذه المكونات و ماذا تفعل .**

١- **Version:** هذه الخانة موجود فيها اصدار بروتوكول الـ **OSPF** و وثيقة البروتوكول و موصفات البروتوكول.

٢- **Type:** هذه الخانة المسؤولة عن شكل حزم البيانات و يتم فيه وصف شكل البيانات مثل:

- **Hello Packets** رسالة الترحيب.
- **Data base Description** وصف قاعدة البيانات.
- **Link State Request** طلب الربط ما بين الراوترات.
- **Link State Update** ربط حالة التحديثات.
- **Link State Acknowledgment** ربط حالة الاستقرار في عملية التاكيد.

٣- **Packet Length:** هذه الخانة المسؤولة عن طول وحجم حزمة بروتوكول **OSPF** في الـ **Header**.

٤- **Router ID:** هذه الخانة المسؤولة عن توجيه مصدر الحزمة في بروتوكول الـ **OSPF** بمعنى إنها تقوم بإرسال حزم البيانات للراوتر المطلوب.

٥- **Area ID** : هذه الخانة المسؤولة عن رقم المنطقة التي يتوجد فيها الراوترات و التي تخضع تحت منطقة واحدة و تعرف برقم **ID** معين ليتم التعرف عليها .

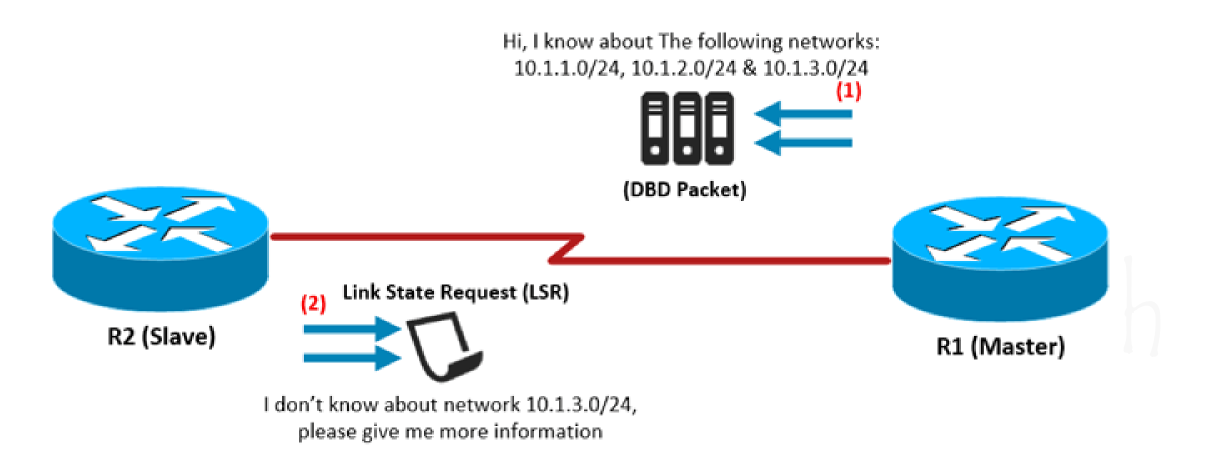
٦- **Checksum:** هذه الخانة المسؤولة عن عملية الفحص.

٧- **AuType** : هذه الخانة هي المسؤولة عن عملية تحديد نوع المصداقية مثل التشفير و كلمات المرور و التوثيق و تقوم هذه الخانة ايضاً بتحقق من عملية التشفير ما بين الطرفين و هل كلمات المرور مشفرة أو لا.

٨- **Authentication:** هذه الخانة تعتمد على النوع الأول بعد عملية الاستقرار و تحديد النوع الذي سيتم فيه عملية التشفير ستقوم هذه الخانة باستخدامه و الاعتماد عليه.

٩- **Data** : هذه الخانة المسؤولة عن الداتا و هي آخر خانة من الخانة بعد تجميع و الحصول على جميع المعلومات سيتم تركيب الداتا في هذه الخانة ليتم ارساله الى الشبكة المطلوبة بشكل صحيح .

٣- **LSR = Link State Request :** هي حزم من البيانات تحتوي على طلب معلومات للوصول لشبكة اخرى يفصل ما بينهم عدة مجموعة راوترات , مثل عندما ا يرد راوتر في شبكة معينة إرسال بيانات لشبكة اخرى سيقوم الراوتر في هذه الحالة بإرسال رسالة **LSR** للراوترات الآخر اقصد في الآخرى الجيران راوترات الجيران ستصل الرسالة إلى أحد الراوترات سيقوم بنظر في داخل معلوماته و قاعدة البيانات الخاصة به إذا وجدة الشبكة المرادة سيقوم بإرسال حزمة البيانات اليها و إذا لم يجد الشبكة المرادة سيقوم بعمل إرسال طلب معلومات إلى راوترات اخرى و يسال الراوتر الآخر هل لديك هذه الشبكة أو هل تعرف مسار هذه الشبكة في هذه الحالة تسمى هذه العملية الربط ما بين راوترات الجيران **LSR** وايضاً عند اكتشاف أن بعض الراوترات لديه قاعدة بيانات لم تتم تحديثها سيقوم الراوتر بإرسال طلب ربط لعمل تحديث على قاعدة البيانات و الطوبولوجي الخاص في الشبكة .



محتويات رسالة طلب الربط LSR: في البداية هذه الرسالة تتكون من **Header** حجم هذا الـ **Header 32 Bit** يتكون من عدة خانات يتم تركيبها بشكل منظم من اعلى إلى اسفل هذا الـ**Header** يحتوي على معلومات الربط ما بين الراوترات لمعرفة مسارات الشبكات و طريقة الربط ما بين الشبكات من خلال طلب الربط **LSR**.

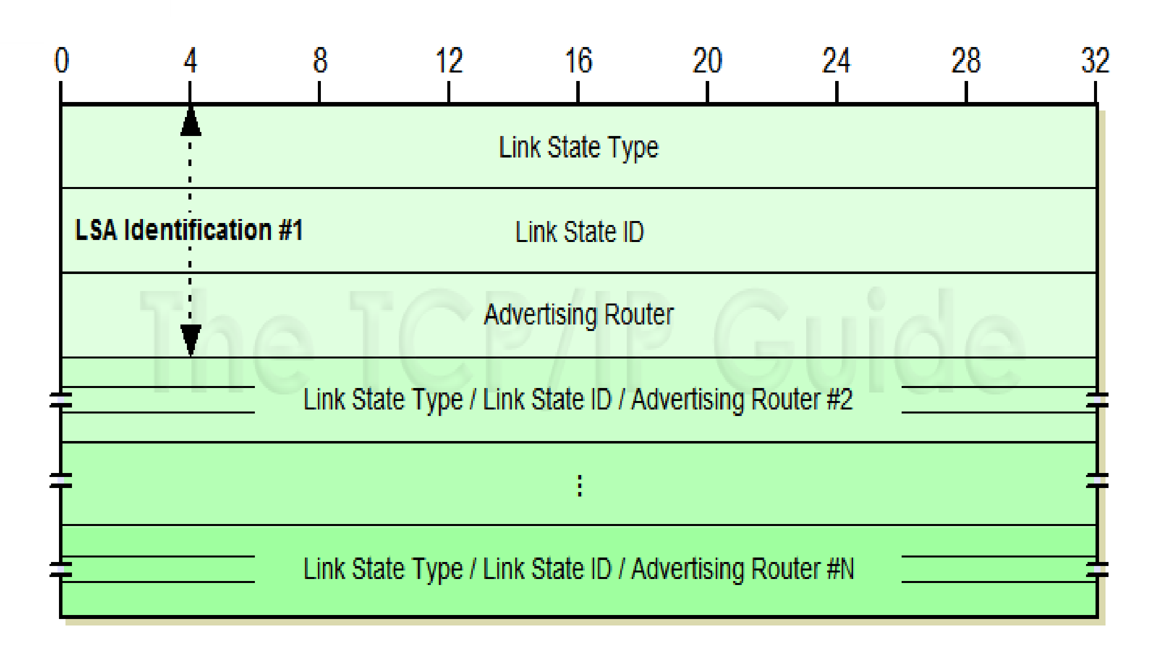
- **الأن سأقوم بذكر محتويات الـ Link State Request الذي تكون في داخل رسالة الـ LSR :**

1-Link State Type

2-Link State ID

3-Advertising Router

كما في النموذج التالي



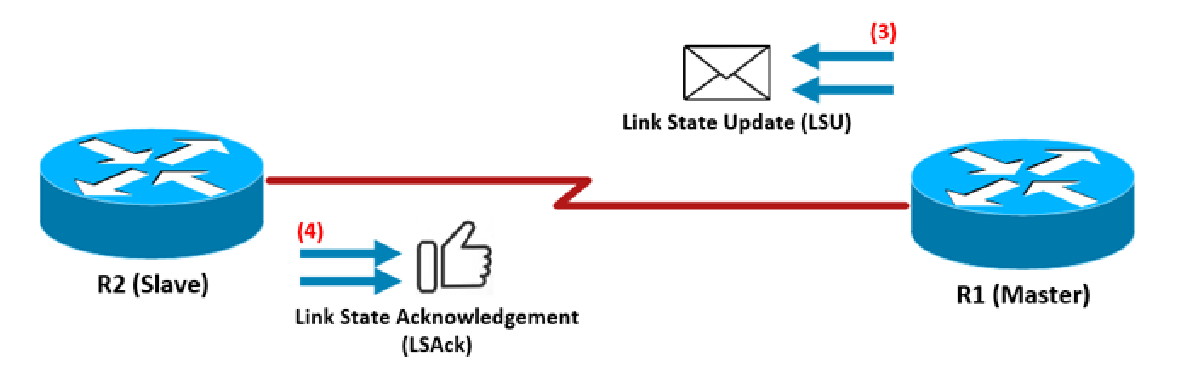
١- **Link State Type:** أنواع حالة الربط يوجد ثلاث أنواع يتم الاعتماد عليهم في حالة الربط ما بين الراوترات ليتم عملية الربط بشكل صحيح.

- جدول قاعدة البيانات **LSDB** يجب أن يكون محدث و إذا لم يكن محدث سيتم ارسل طلب ربط لتحديث قاعدة البيانات من الراوترات الآخر .
- جدول التوجيه و المسارات **Routing Table** يجب أن يكون ايضاً محدث و تم إضافة جميع الشبكات فيه .
- جدول الجيران **Neighbor Table** بمعنى الراوترات المجاورة يجب أن يكون جداول التوجيه الخاصة بهم محدثه ايضاً.

٢- **Link State ID:** يقوم بتحديد حالة الربط بعنوان الراوتر الذي سيتم الإرسال و الاستقبال منه.

٣- **Advertising Router:** بعد الانتهاء من عملية الربط و التحديثات في الراوتر المطلوب سيقوم بعملية الاعلان عن التعديل و التحديثات التي تمت عليه للراوترات الآخر ليتم الاتصال به و العمل بشكل صحيح.

٤- **LSU = Link State Update:** هذه الرسالة اختصار لـ **Link State Advertisemant** و وظيفة هذه الرسالة أن تقوم بعملية اعلان عن محتويات الشبكة الخاص في **OSPF** و يتم إرساله في داخل الـ **LSU**.

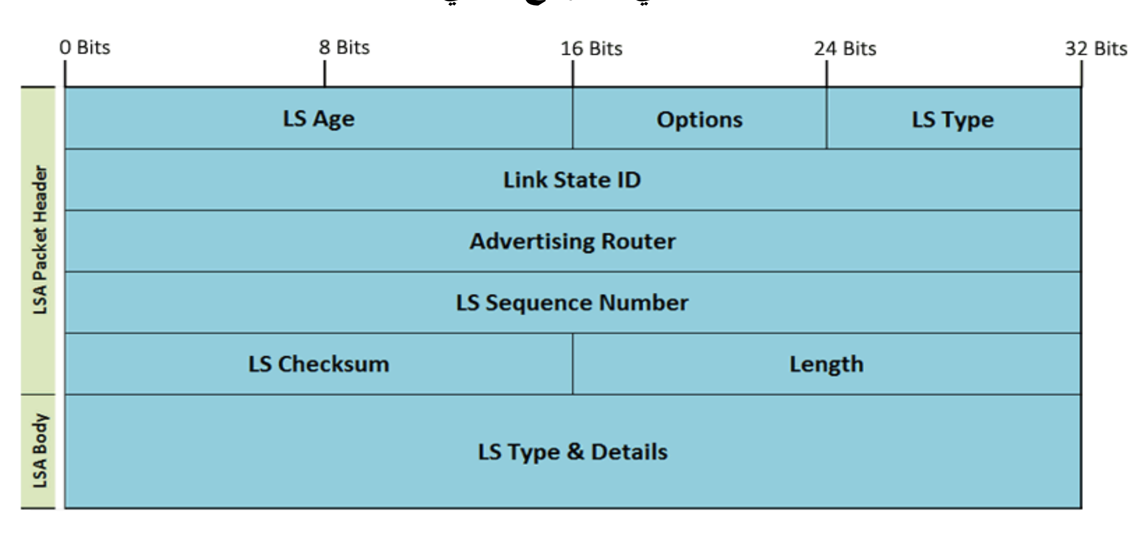


محتويات رسالة الاعلان عن المحتويات LSU: في البداية هذه الرسالة تتكون من **Header** حجم هذا الـ **Header 32 Bit** يتكون من عدة خانات يتم تركيبها بشكل منظم من اعلى إلى اسفل .

- **الأن سأقوم بذكر محتويات الـ Link State Update الذي تكون في داخل رسالة الـ LSU :**

1- **LS Age**
2- **Options**
3- **LS Type**
4- **Link State ID**
5- **Advertising Router**
6- **LS Sequence Number**
7- **LS Checksum**
8- **Length**
9- **LSA body / LS type**

كما في النموذج التالي



- **الأن سأقوم بشرح كل واحدة من هذه المكونات بشكل منفرد عن الآخر لنفهم وظيفة كل واحدة من هذه المكونات و ماذا تفعل .**

١- **LS Age :** وظيفة هذه الخانة تنظيم الوقت و الزمان من بداية انشاء الـ **LSA** و حجم هذه الخانة **2 bits** .

٢- **Options** : هذه خانة الخيارات تقوم بتكوين مميزات **OSPF** و اختيار افضل خيار لبروتوكول الـ **OSPF** ليتمكن من دعم الخانة الآخر و حجم هذه الخانة **1 bits**.

٣- **LS Type :** هذه الخانة المسؤولة عن تحديد أنواع الـ **LSA** و سأقوم بذكرهم لاحقاً وحجم هذه الخانة **1 bits**.

٤- **Link State ID** : هذه الخانة المسؤولة عن الربط ما بين الراوترات و الشبكات التي تعمل في بروتوكول الـ **OSPF** و تعتمد هذه الخانة على عنوان الاي بي **IP** و وحجم هذه الخانة من **4 bits**.

٥- **Advertising Router**: هذه الخانة المسؤولة عن اعلان الراوتر بعنوان الاي بي **IP** الخاص في الراوتر الاصلي و حجم هذه الخانة **4 bits**.

٦- **LS Sequence Number :** هذه الخانة المسؤولة عن عدد الـ **LSA** و يتم التحديد لكل رسالة **LSA** برقم لتقوم بعملية التصفية و تبين الرسالة القديمة من الجديدة أو المتكررة و حجم هذه الخانة **4 bits**.

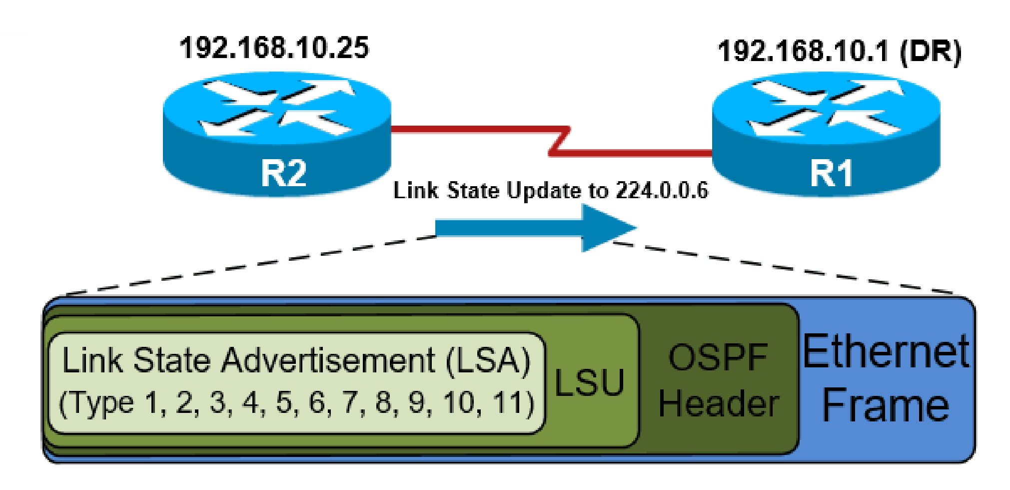
٧- **LS Checksum**: هذه الخانة المسؤولة عن اختبار الـ **LSA** و تقوم بترقيم الـ **LSA** للمقارنة و اكتشاف الاخطاء.

٨- **Length** : هذه الخانة هي المسؤولة عن طول حزمة الـ **LSA** و تحديد طولها.

٩- **LSA body / LS type**: هذه الخانات المسؤولة عن عن مكونات الـ **LSA** و أنواع الـ **LSA** هذه الطبقة تاتي ما بعد تكوين الطبقة الأولى **LSA Packet Header** بعد تكون هذه الطبقة سياتي دور الـ **LS type** / **LSA body** و يتم فيه عملية التكوين الخاصة في **LSA** .

- هاكذا يكون تم الانتهاء من الشرح **LSU** و اريد أن اقوم بشرح أنواع الـ **LSA** التي تتكون في داخل الـ **Link State Advertisemant** و يتجاوز عدد هذه الأنواع ما يقارب الـ **11** نوع من أنواع الـ **LSA** الأن سأقوم بذكر و شرح هذه الأنواع .

Types of link-state advertisements



LSA Type 1 = Router LSA

LSA Type 2 = Network LSA

LSA Type 3 = Summary LSA = ABR LSA

LSA Type 4 = Summary LSA = ASBR LSA

LSA Type 5 = External LSA

LSA Type 6 =Multicast OSPF LSA

LSA Type 7 = External LSA for NSSA

LSA Type 8 = External Attributes

LSA Type 9 = Intra – Area – Prefix

LSA Type 10 = Area – Local – Opaque

LSA Type 11 = AS Opaque

- **الأن سأقوم بشرح كل واحدة من هذه الأنواع بشكل منفرد عن الآخر لنفهم وظيفة كل واحدة من هذه المكونات و ماذا تفعل و على ماذا تحتوي :**

- **LSA Type 1 = Router LSA:** وظيفة هذا النوع من الـ **LSA** يقوم الراوتر بإرسال وصف من البيانات الموجودة في هذه النوع من الـ **LSA** و يقوم بالرساله للراوترات المجاورة على الإنترفيس المتصلة فيه.

- **LSA Type 2 = Network LSA :** وظيفة هذا النوع من الـ **LSA** ترسل فقط للشبكات التي تعمل في البث المباشر **broadcast** و المتصلة في الراوترات بشكل مباشر بمعنى أن تكون الراوترات في شبكة واحد متصلة مع بعضها البعض .

- **LSA Type 3 = Summary LSA = ABR LSA :** في هذا النوع تتم عملية مهمة جداً جداً و هي أن يقوم جهاز الراوتر بعملية لمس للمناطق **Area** بشكل متعددة من الشبكة لعملية تلخيص كاملة عن المعلومات مره واحد مثل يكون عنوان و تحت هذا العنوان يوجد اكثر من عنوان بنفس المبداء في هذه الحالة تقوم هذه الرسالة باخذ العنوان الرئيسي يقوم بعملية لمس و معرفة المعلومات مره واحدة من المنطقة **Area** التي يريد منها الراوتر معرفة المعلومات ليقوم بعملية تحديث .

- **LSA Type 4 = Summary LSA = ASBR LSA :** وظيفة هذا النوع يحتاج لمعرفة المسارات الآخر لمعرفة اين يجد راوتر الـ **ASBR** و لهذا السبب يتظمن عنوان الـ **Router ID ABR** ليتمكن من معرفة مسار الـ **ASBR** .

- **LSA Type 5 = External LSA :** و ظيفة هذا النوع تحديد طريق الخروج للشبكة الخارجية و هذا النوع من الرسال يعتمد على الإرسال من خلال جهاز الراوتر الموجود على حدود الـ **Area** ليقوم بوصفها من اي طريق يخرج أو يتصل في الشبكة الخارجية من خلال الراوتر الموجود على حدود الـ **Area** على سبيل المثال الراوتر المتصل في الانترنت.

- **LSA Type 6 =Multicast OSPF LSA :** هذا النوع غير مدعوم و غير مستعمل فهو قديم جداً .

- **LSA Type 7 = External LSA for NSSA :** هذا النوع هو عبارة عن قائمة من المعلومات تستخدم في الشبكات الخارجية لشبكة الـ **OSPF** .

- **:LSA Type 8 = External Attributes** هذا النوع كان يستخدم لنقل وصلة خصائص بروتوكول الـ **BGP** إلى شبكة الـ **OSPF** لكن لم تعد تستخدم بكثرة في بروتوكول الـ **OSPF** ولكن في الإصدار الثالث من بروتوكول **OSPFv3** هو مصمم لإرسال المعلومات إلى **IPv6 address** ليتم الربط بعنوان الشبكة محلية.

- **LSA Type 9 = Intra – Area – Prefix :** هذه الخانة وظيفتها بداية تكوين معلومات الشبكة الداخلية و معرفة المنطقة التي في داخلها .

- **:LSA Type 10 = Area – Local – Opaque** وظيفة هذا النوع أن يستمر في إرسال المعلومات إلى مسار المنطقة حتى لو كان المسار لا يفهم المعلومات من قبل التطبيقات ولكن سيتم إرسال هذه الوظيفة لبروتوكول الـ **OSPF**.

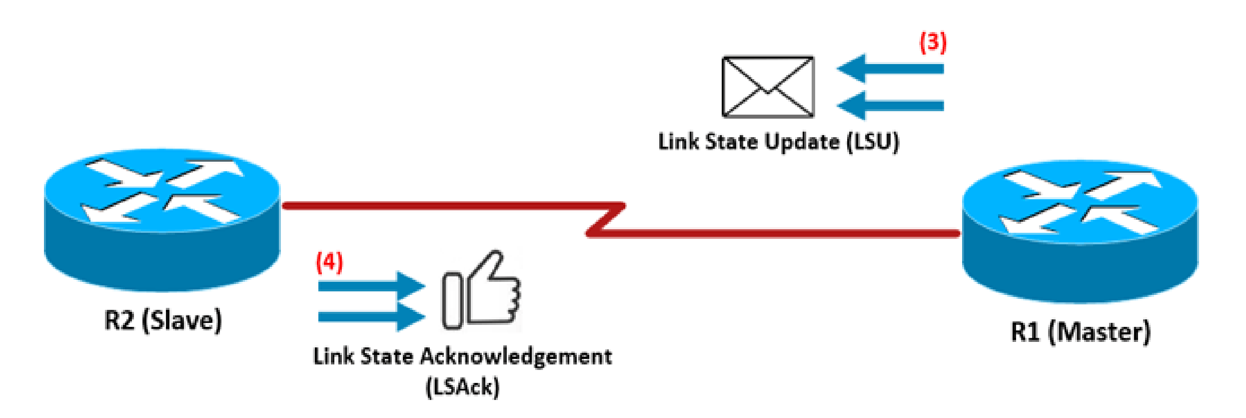
- **LSA Type 11 = AS Opaque : هذه آخر نوع من الانواع ولان نحتاج له الا في الوقت الحالي و سنتعرف عليها اكثر في مستوى المحترفين .**

- **هاكذا يكون قد تم شرح الـ 11 نوع و ولكن في الحقيقة يتم الاعتماد فقط على 7 أنواع اساسية يتم العمل فيه و باقي الأنواع تكون موجودة ايضاً ولكن لا يتم استخدامه كثيراً مثل الـ 7 أنواع التالية التي يتم الاعتماد عليه بشكل رسمي كما في الجدول التالي:**

LSA	Generated by	Function	Flooding Map
Type 1	Normal Area Routers	Advertising router's interface and status to neighbors	Intra-Area (Area of origin)
Type 2	DR	Advertising DRs direct connected neighbors	Intra-Area (Area of origin)
Type 3	ABR	Advertising ABRs areas summary	Inter-Area (Multiple Areas)
Type 4	ABR	Advertising the presence of ASBRs	Inter-Area (Multiple Areas)
Type 5	ASBR	Advertising external routes to internet	Inter-Area (Multiple Areas)
Type 7	ASBR	Advertising external routes to internet to NSSA areas	Inter-Area (Multiple Areas)

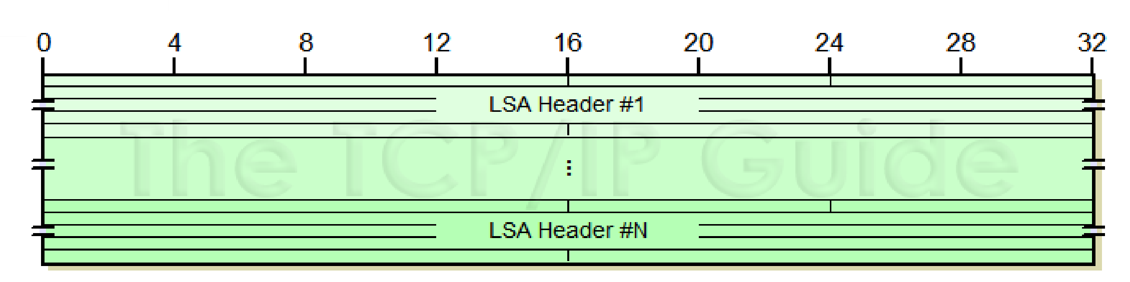
- **و بهذا الشكل يكون قد تم الانتهاء من ذكر و شرح جميع الأنواع الخاصة في أنواع الربط Types of link-state advertisements .**

٥- **LSAck = Link State Acknowledgement:** هذه رسالة التاكيد على عملية إستلام و تبادل المعلومات بشكل صحيح و تحتوي على خمسة أنواع من القيم الخاصة في الـ **header** تحتوي على قائمة عناوين **LSA headers** و على المقابل يتم تركيبهما لتتم عملية القراءة من **LSA** و بعده سيتم التاكيد على الاستلام بالرد بعنوان الـ **LSA headers** المطابقة لها نفسها لتصبح جميع الراوترات تعمل بنفس قاعدة البيانات.



محتويات رسالة التاكيد على اسلام التحديثات LSAck: في البداية هذه الرسالة تتكون من **Header** حجم هذا الـ **Header 32 Bit** يتكون من خانتين فقط يتم تركيبهم بشكل منظم من اعلى إلى اسفل .

كما في النموذج التالي



- **هكذا يكون قد تم الانتهاء بشكل كامل من شرح أنواع حزم بيانات بروتوكول الـ OSPF**

- اريد أن اقوم بتوضيح بعض التفاصيل بخصوص موضوع حزم البيانات و اريد أن اقوم بعرض تفاصيل البيانات و هاي ترسل في الشبكة التي لا نستطيع أن نرها و تكون في خلفية الشبكة **background network**.
- سيتم الشرح على طوبولوجي مبني من قبل و لا نريد التطبيق عليه ولا نريد العمل عليه فقط نريد الدراسة و الشرح عليه و معرفة البيانات كيف تسير في خلفية الشبكة ما بين الراوترات ؟

هذا هو الطوبولوجي

- **في هذه الطوبولوجي نريد أن نشرح تنقل الحزم ما بين الراوتر التي تكون في خلفية الشبكة.**
- الأن إذا نظرنا على الطوبولوجي سنرى اكثر من راوتر في الطوبولوجي سنقوم بشرح و تفصيل الحزمة التي تمر ما بين **R1** و **R2** و نرى كيف تتم هذه العملية و ما هي الحزم التي تنتقل في اثناء النقل سنقوم بعرض هذه التفاصيل على أحد برامج مراقبة الشبكة لا اريد أن اذكر ما هو البرنامج في الوقت الحالي لي إنه يحتاج شرح و معرفة للعمل عليه سأقوم فقط بشرح التفاصيل التي تظهر في عملية النقل و في الدروس القادمة سأقوم بذكر اسم البرنامج و كيفية العمل عليه بالتفصيل تابع الشرح .

- أنظر هذه أول صورة لعملية نقل الحزم و هذه حزمة رسالة الترحيب الـ **Hello Packets** في خلفية الشبكة أنظر كيف تتم عملية بناء الـ **OSPF Header**.

```
⊞ Frame 47: 90 bytes on wire (720 bits), 90 bytes captured (720 bits) on interface 0
⊞ Ethernet II, Src: c2:08:19:b8:00:00 (c2:08:19:b8:00:00), Dst: IPv4mcast_00:00:05 (01:00:5e:00:00:05)
⊞ Internet Protocol Version 4, Src: 10.0.0.4 (10.0.0.4), Dst: 224.0.0.5 (224.0.0.5)
⊟ Open Shortest Path First
  ⊟ OSPF Header
      OSPF Version: 2
      Message Type: Hello Packet (1)
      Packet Length: 44
      Source OSPF Router: 0.0.0.4 (0.0.0.4)
      Area ID: 0.0.0.0 (Backbone)
      Packet Checksum: 0xeba2 [correct]
      Auth Type: Null
      Auth Data (none)
  ⊟ OSPF Hello Packet
      Network Mask: 255.255.255.248
      Hello Interval: 10 seconds
    ⊟ Options: 0x12 (L, E)
        0... .... = DN: DN-bit is NOT set
        .0.. .... = O: O-bit is NOT set
        ..0. .... = DC: Demand Circuits are NOT supported
        ...1 .... = L: The packet contains LLS data block
        .... 0... = NP: NSSA is NOT supported
        .... .0.. = MC: NOT Multicast Capable
        .... ..1. = E: External Routing Capability
        .... ...0 = MT: NO Multi-Topology Routing
      Router Priority: 1
      Router Dead Interval: 40 seconds
      Designated Router: 0.0.0.0
      Backup Designated Router: 0.0.0.0
  ⊟ OSPF LLS Data Block
      Checksum: 0xfff6
      LLS Data Length: 12 bytes
    ⊟ Extended options TLV
        Type: 1
        Length: 4
      ⊟ Options: 0x00000001 (LR)
          .... .... .... .... .... .... .... ..0. = RS: Restart Signal (RS-bit) is NOT set
          .... .... .... .... .... .... .... ...1 = LR: LSDB Resynchronization (LR-bit) is SET
```

- لاحظ في الصورة إنه يتم جمع المعلومات و يقوم ايضاً بنظر على معلومات و إعدادات الشبكة و البروتوكول ، مثل الـ **Router Dead Interval : 40 seconds** هذا الوقت الخاص في رسالة الترحيب في حال لم يتم الرد خلال الـ **40** ثانية سيتم الغاء العملية و الغاء الاتصال ما بيت الراوتر .

- الأن بعد وصول رسالة الترحيب لـ **R2** سيتم عودة إرسال حزمة قاعدة البيانات **DBD** لعملية تحديث قاعدة البيانات في الـ **R2** كم في الصورة التالية :

```
⊞ Frame 19: 158 bytes on wire (1264 bits), 158 bytes captured (1264 bits) on interface 0
⊞ Ethernet II, Src: c2:05:19:b8:00:00 (c2:05:19:b8:00:00), Dst: c2:06:19:b8:00:00 (c2:06:19:b8:00:00)
⊞ Internet Protocol Version 4, Src: 10.0.0.1 (10.0.0.1), Dst: 10.0.0.2 (10.0.0.2)
⊟ Open Shortest Path First
  ⊟ OSPF Header
      OSPF Version: 2
      Message Type: DB Description (2)
      Packet Length: 112
      Source OSPF Router: 0.0.0.1 (0.0.0.1)
      Area ID: 0.0.0.0 (Backbone)
      Packet Checksum: 0x7f8e [correct]
      Auth Type: Null
      Auth Data (none)
  ⊞ OSPF DB Description
  ⊟ LSA Header
      LS Age: 612 seconds
      Do Not Age: False
    ⊞ Options: 0x22 (DC, E)
      Link-State Advertisement Type: Router-LSA (1)
      Link State ID: 0.0.0.1
      Advertising Router: 0.0.0.1 (0.0.0.1)
      LS Sequence Number: 0x80000041
      LS Checksum: 0x28b2
      Length: 36
  ⊟ LSA Header
      LS Age: 786 seconds
      Do Not Age: False
    ⊞ Options: 0x22 (DC, E)
      Link-State Advertisement Type: Router-LSA (1)
      Link State ID: 0.0.0.4
      Advertising Router: 0.0.0.4 (0.0.0.4)
      LS Sequence Number: 0x80000026
      LS Checksum: 0xfde4
      Length: 36
  ⊟ LSA Header
      LS Age: 612 seconds
      Do Not Age: False
    ⊞ Options: 0x22 (DC, E)
      Link-State Advertisement Type: Network-LSA (2)
      Link State ID: 10.0.0.1
      Advertising Router: 0.0.0.1 (0.0.0.1)
      LS Sequence Number: 0x80000026
      LS Checksum: 0xda30
      Length: 32
  ⊟ LSA Header
      LS Age: 791 seconds
      Do Not Age: False
    ⊞ Options: 0x22 (DC, E)
      Link-State Advertisement Type: Summary-LSA (IP network) (3)
      Link State ID: 10.0.0.12
      Advertising Router: 0.0.0.4 (0.0.0.4)
      LS Sequence Number: 0x80000001
      LS Checksum: 0x6eb6
      Length: 28
  ⊞ OSPF LLS Data Block
```

- لاحظ إنه يتم بناء الـ **OSPF Header** ويتم النزول من اعلى إلى اسفل و يبداء في بناء الـ LSA بشكل مرتب و حسب النوع أنظر جيداً للصورة اعلى لتفهم كيف تتم عليمة البناء , تتم عملية البناء على الشكل التالي حيث يتم جمع كافة المعلومات المطلوبة مثل الاي بي و عنوان المنطقة و نوع الربط المطلوب , لاحظ ايضاً أن بروتوكول الـ **OSPF** يعتمد اعتماد كبير على بروتوكول الانترنت **IPv4** حيث يتم فيه تحديد اي بي المرسل **Src 10.0.0.1** و اي بي المستقبل **Dst 10.0.0.2** .
- لاحظ إنه تم تحديد ثلاث أنواع من حزم البيانات **LSA Type 1 , LSA Type 2 , LSA Type 3** .

- الأن بعد أن تم استلام R2 رسالة الـ **DBD** من **R1** و قام بعملية التحديث في قاعدة البيانات سيتم إرسال رسالة الـ **LSR** لـ **R1** لمعرفة المسارات و الراوترات التي تم التعرف عليها من خلال **R2** .

```
⊞ Frame 24: 106 bytes on wire (848 bits), 106 bytes captured (848 bits) on interface 0
⊞ Ethernet II, Src: c2:06:19:b8:00:00 (c2:06:19:b8:00:00), Dst: c2:05:19:b8:00:00 (c2:05:19:b8:00:00)
⊞ Internet Protocol Version 4, Src: 10.0.0.2 (10.0.0.2), Dst: 10.0.0.1 (10.0.0.1)
⊟ Open Shortest Path First
  ⊟ OSPF Header
      OSPF Version: 2
      Message Type: LS Request (3)
      Packet Length: 72
      Source OSPF Router: 10.0.0.9 (10.0.0.9)
      Area ID: 0.0.0.0 (Backbone)
      Packet Checksum: 0xdf88 [correct]
      Auth Type: Null
      Auth Data (none)
  ⊟ Link State Request
      Link-State Advertisement Type: Router-LSA (1)
      Link State ID: 0.0.0.1
      Advertising Router: 0.0.0.1 (0.0.0.1)
  ⊟ Link State Request
      Link-State Advertisement Type: Router-LSA (1)
      Link State ID: 0.0.0.4
      Advertising Router: 0.0.0.4 (0.0.0.4)
  ⊟ Link State Request
      Link-State Advertisement Type: Network-LSA (2)
      Link State ID: 10.0.0.1
      Advertising Router: 0.0.0.1 (0.0.0.1)
  ⊟ Link State Request
      Link-State Advertisement Type: Summary-LSA (IP network) (3)
      Link State ID: 10.0.0.12
      Advertising Router: 0.0.0.4 (0.0.0.4)
```

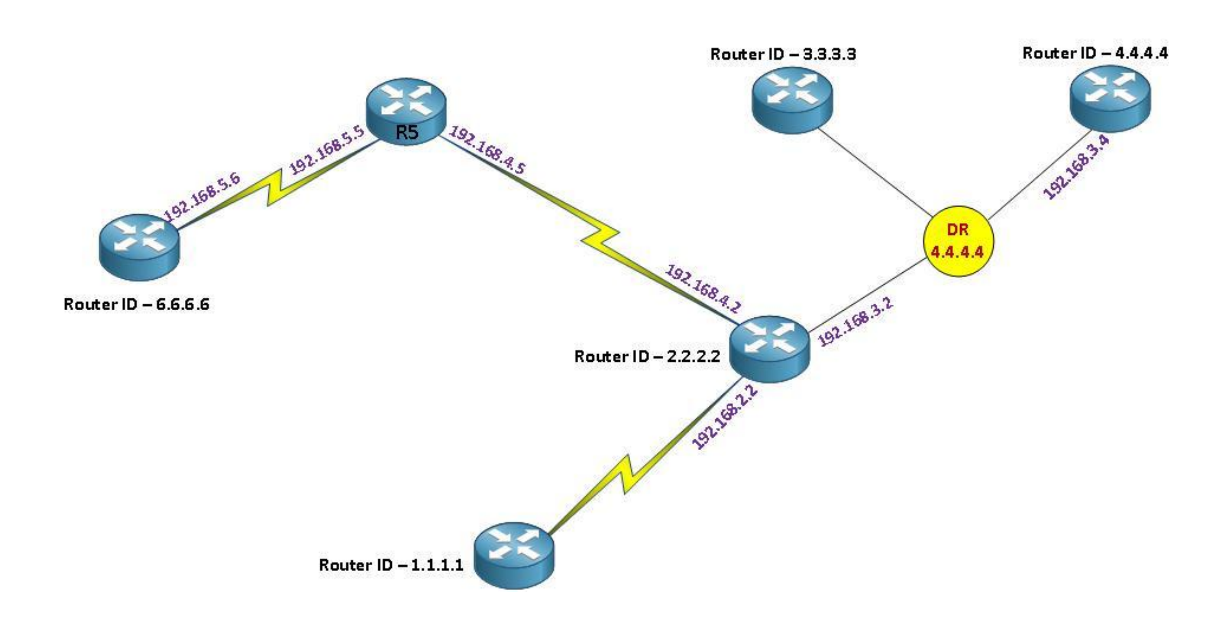

- لاحظ نه تم إرسال ثلاث أنواع من رسالة الـ **LSA** كل واحدة منهم تحمل معلومات مختلفة عن الآخر و سبق أن شرحنا هذ الأنواع .
- الأن في هذه الحالة **R2** سيقوم بطلب معلومات تحديث اخرى خاصة في **LSA** سياتي دور رسالة الـ **LSU** .

```
⊞ Frame 26: 194 bytes on wire (1552 bits), 194 bytes captured (1552 bits) on interface 0
⊞ Ethernet II, Src: c2:05:19:b8:00:00 (c2:05:19:b8:00:00), Dst: c2:06:19:b8:00:00 (c2:06:19:b8:00:00)
⊞ Internet Protocol Version 4, Src: 10.0.0.1 (10.0.0.1), Dst: 10.0.0.2 (10.0.0.2)
⊟ Open Shortest Path First
  ⊟ OSPF Header
      OSPF Version: 2
      Message Type: LS Update (4)
      Packet Length: 160
      Source OSPF Router: 0.0.0.1 (0.0.0.1)
      Area ID: 0.0.0.0 (Backbone)
      Packet Checksum: 0xb899 [correct]
      Auth Type: Null
      Auth Data (none)
  ⊟ LS Update Packet
      Number of LSAs: 4
    ⊟ LS Type: Router-LSA
        LS Age: 614 seconds
        Do Not Age: False
      ⊞ Options: 0x22 (DC, E)
        Link-State Advertisement Type: Router-LSA (1)
        Link State ID: 0.0.0.1
        Advertising Router: 0.0.0.1 (0.0.0.1)
        LS Sequence Number: 0x80000041
        LS Checksum: 0x28b2
        Length: 36
      ⊞ Flags: 0x00
        Number of Links: 1
      ⊞ Type: Transit  ID: 10.0.0.1         Data: 10.0.0.1         Metric: 1
    ⊟ LS Type: Router-LSA
        LS Age: 787 seconds
        Do Not Age: False
      ⊞ Options: 0x22 (DC, E)
        Link-State Advertisement Type: Router-LSA (1)
        Link State ID: 0.0.0.4
        Advertising Router: 0.0.0.4 (0.0.0.4)
        LS Sequence Number: 0x80000026
        LS Checksum: 0xfde4
        Length: 36
      ⊞ Flags: 0x01 (B)
        Number of Links: 1
      ⊞ Type: Transit  ID: 10.0.0.1         Data: 10.0.0.4         Metric: 10
```

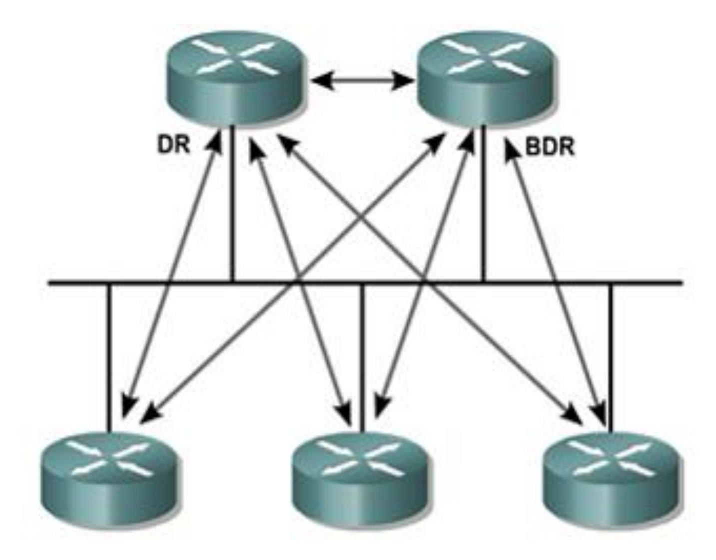
هذه رسالة التاكيد على عملية إستلام و تبادل المعلومات بشكل صحيح و تحتوي على خمس أنواع من القيم الخاصة في الـ **header** تحتوي على قائمة عناوين **LSA headers** و على المقابل يتم تركيبهما لتتم عملية القراءة من **LSA** و بعده سيتم التاكيد على الاستلام بالرد بعنوان الـ **LSA headers** المطابقة لها نفسها لتصبح جميع الراوترات تعمل بنفس قاعدة البيانات.

```
⊟ LS Type: Network-LSA
    LS Age: 614 seconds
    Do Not Age: False
  ⊞ Options: 0x22 (DC, E)
    Link-State Advertisement Type: Network-LSA (2)
    Link State ID: 10.0.0.1
    Advertising Router: 0.0.0.1 (0.0.0.1)
    LS Sequence Number: 0x80000026
    LS Checksum: 0xda30
    Length: 32
    Netmask: 255.255.255.248
    Attached Router: 0.0.0.1
    Attached Router: 0.0.0.4
⊟ LS Type: Summary-LSA (IP network)
    LS Age: 792 seconds
    Do Not Age: False
  ⊞ Options: 0x22 (DC, E)
    Link-State Advertisement Type: Summary-LSA (IP network) (3)
    Link State ID: 10.0.0.12
    Advertising Router: 0.0.0.4 (0.0.0.4)
    LS Sequence Number: 0x80000001
    LS Checksum: 0x6eb6
    Length: 28
    Netmask: 255.255.255.252
    Metric: 1
```

- لاحظ إنه يوجد ما يسمى **Attached Router** هذه العملية تبين لنا إنه تم ملامسة التغير و التحديث في الراوتر المراد تحديث قاعدة البيانات له و بهذه الشبكة تكون الراوترات قد تما تحديث قاعدة البيانات الخاص في الراوتر .



عملية إنتخاب الـ DR and BDR



- **كيف تتم عملية الانتخاب ما بين الراوترات :**

تتم عملية الانتخاب عن طريق عدة خطوات سنقوم بذكرها .

١- **Priority:** تقوم جميع الراوترات بالنظر إلى الأولية الـ **Priority** و تأتي في جميع الراوترات **Priority Default 1** و نستطيع تغيرها و هو عبارة عن رقم يبدا من **0** حتى **255** الراوتر الذي سيأخذ رقم **0** لن يدخل في عملية الانتخاب وسيتم اختيار اعلى قيمة ليكون **DR** والاقل منه سيكون **BDR** مثل لو كان أحد الراوترات يمتلك **Priority Default 1** و الثاني يمتلك القيمة **Priority Default 2** في هذه الحالة سيكون راوتر الـ **DR** من لديه قيمة الـ **Priority Default 2** و الراوتر الذي يمتلك قيمة **Priority Default 1** هو الذي سيكون راوتر الـ **BDR** وفي أن قيمة الـ **Priority Default 1** في جميع الراوترات سيتم تخطى هذه المرحلة و الانتقال لمرحلة الـ **RID** لعملية الانتخاب .

٢- **RID:** هو اختصار لـ **Router ID** و تاتي وظيفته بعد قيمة الـ **Priority** سيتم الانتقال إلى **RID** و هو عبارة عن عنوان من الإصدار الرابع و يقوم مهندس الشبكة بعمل إعدادات على جهاز الراوتر المفعل عليه بروتوكول الـ **OSPF** ليتم التعريف بنفسه لباقي الراوترات المفعل عليها بروتوكول **OSPF** يتم تركيب الاي بي و هو العنوان الذي من الإصدار الرابع طبعاً و سنقوم بعمل مثال لو لدينا في الشبكة عدة راوترات الراوتر الأول تم تركيب الاي بي **10.10.10.10** و الراوتر الثاني تم تركيب الاي بي **11.11.11.11** من الذي سيكون **DR** من الطبيعي جداً الراوتر الذي يمتلك **Router ID** اعلى و هو **11.11.11.11** و هو الراوتر الثاني في هذه الحالة سيتم اعطاء الراوتر الثاني مسؤلية الـ **DR** و الراوتر الأول سيقوم باخذ مسؤالية **BDR** و إذا لم يتم التطابق بهذه المرحلة سيتم الاتنتقال للمرحلة الآخر .

٣- **Loopback IP Address:** هو المنفذ الوهمي الذي يكون على جهاز الراوتر يستخدم في حالة استكشاف المشاكل و الاعطال في جهاز الراوتر في حال توقف الراوتر عن العمل و الإنترفيس لا يعمل سنقوم بعملية اختبار للمنفذ الوهمي لنتاكد من سلامة الراوتر، و يستخدم هذا المنفذ في عملية الانتخاب في حال إنه ياخذ اعلى انترفيس في جهاز الراوتر بشكل وهمي إذا لم يجد الإنترفيس الحقيقي مثل نقوم بتفعيل الإنترفيس الوهمي و نقوم بتركيب الاي بي عليه **100.100.100.100** و يوجد انترفيس ثاني وهمي ايضاً يمتلك اي بي **200.200.200.200** من الطبيعي سيقوم سيقوم باخذ الإنترفيس الاعلى و في هذه الحالة سيتم اختيار راوتر الـ **DR** و **BDR** و إذا لم تتم هذه المرحلة سينتقل للمرحلة الآخر .

٤- **High Physical Interface:** هذه الحالة في حال لم يتعرفر على جميع ما ذكر من قبل سيقوم بذهب إلى اعلى انترفيس في الراوتر مثل سرعة الإنترفيس **fastehternet** أو **giga ethernet** الذي يعمل عليه بروتوكول الـ **OSPF** و يقوم بتعنيها لعملية انتخاب راوتر الـ **DR** و **BDR** وهي آخر مرحلة تتم في عملية الخطوات.

- الأن بعد الانتهاء من شرح خطوات عملية الانتخاب ما بين الراوترات يجب أن نعرف أن هذه الخطوات لا يتم احتيجها الا في حال حدوث مشكلة في الراوتر الرئيسي الـ **DR** ويجب المعرفة أن راوتر الـ **DR** يتم انتخابه عن طريق أول راوتر يتم تركيبه على الشبكة ويتم تفعيل بروتوكول الـ **OSPF** عليه هو من ياخذ الراوتر الرئيسي **DR** طبعاً في الشبكة السريعة مثل شكبة البث المباشر **Broadcast** التي تكون في نطاق واحد أو على سوتيش واحد .

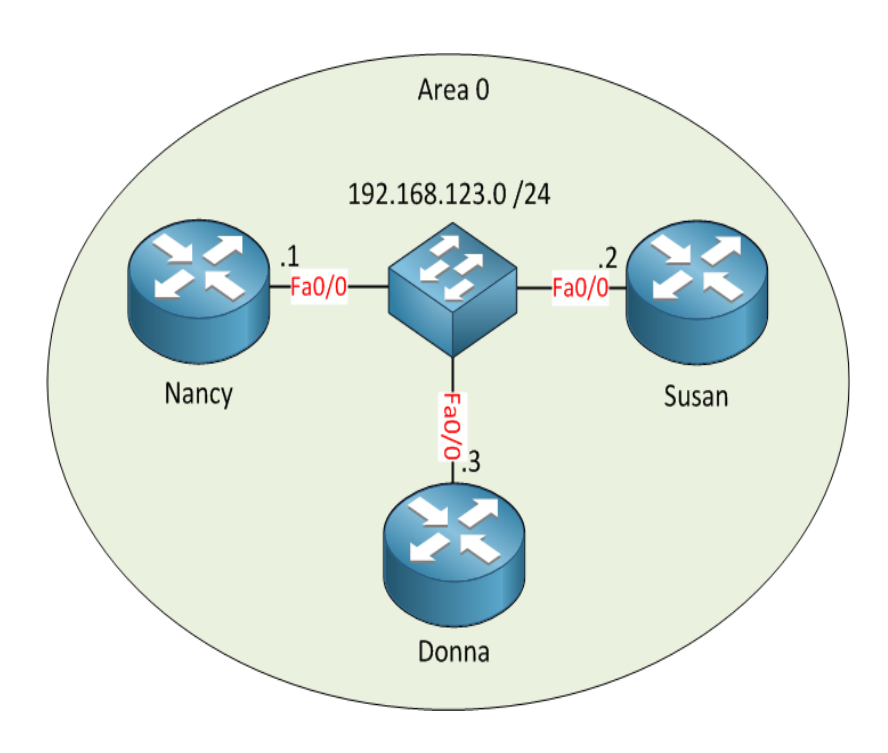
ملاحظة : هذه العملية تعمل على شبكة من نوع **BMA** بمعنى إنهم الراوترات المتصلين في جهاز سوتيش واحد و بنفس الشبكة اما بنسبه للشبكة التي تعمل في نطاق **Frame Relay** أو شبكة الـ **PPP** تقوم بتعين الراوتر الرئيسي لوحده و كل راوتر في الشبكة ياخذ تعين لنفسه **DR** لي إنهم مختلفين في نطاق الشبكة و ليسوا على شبكة في نطاق واحد مثل الـ **BMA**.

- **DRother :** هي الراوترات التي لا تكون في عملية الانتخابات لا **DR** و **BDR** و تكون هذه الحالة ما بين الراوترات التي تكون في حالة **DRother** تكون حالة الـ **Two Way State** , اما في حالة **DR** و **BDR** تكون الحالة **Full State** .

- العناوين الخاصة في بروتوكول الـ **OSPF** يوجد نوعان واحد يتم استخدامه في ما بين الراوترات الـ **DR** و **BDR** و الثاني يتم استخدمه في راوترات الـ **DRother** .

- **224.0.0.5: من خلال هذا العنوان راوترات الـ DRother تستطيع الاتصال مع بعضها البعض.**
- **224.0.0.6: من خلال هذا العوان راوترات الـ DR و BDR تستطيع الاتصال مع بعضها البعض .**

- مثال على بروتوكول الـ **OSPF** ولماذا لديه عملية انتخاب للراوترات **DR** و **BDR** الأن لنعتبر أن لدينا شركة عملاقة و في داخل الشركة تم بناء شبكة ضخمة جداً في هذه الحالة من الطبيعي أن نحتاج راوترات و معدة اخرى سنقوم بعمل شبكة الراوترات وسنقوم بتفعيل بروتوكول الـ **OSPF** على الراوترات من الطبيعي أن نقوم ببناء شبكة الراوترات بعددة اشكال اما في هذا المثال نريد أن نقوم بعمل شبكة في نطاق واحد مثل يوجد لدينا اربعة راوترات متصلة بسوتيش واحد و تعمل في نطاق واحد سنقوم بوضع العناوين و ستقوم عملية الانتخاب من الذي سيكون الراوتر الرئيسي و الراوتر الاحتياطي لنقول إنه تمت عملية الانتخاب بشكل صحيح بعد هذا سنقول ما فائدة عملية الانتخاب و ما هي الفائدة من عملية تعين راوتر رئيسي و راوتر احتياطي في هذه الحالة يجب أن نعلم أن جميع الشبكات الموجود في داخل الشركة تعتمد على هذه الراوترات و من الطبيعي إنه يوجد ضغط كبير على هذه الراوترات هنا تاتي فائدة وجود اكثر من راوتر و عملية الانتخاب لنفترض إنه تم اختراق أو أو ايقاف الراوتر الرئيسي الذي يدير الشبكة كلها في هذه الحالة سيتم ايقاف الشبكة كلها عن العمل أن لم يكون راوتر احتياطي هنا تاتي وظيفة الراوتر الاحتياطي ليقوم بدور الراوتر الرئيسي و يقوم ايضاً بتوزيع الترافيك بمعنى توزيع الحمل على الرواترات ليتم العمل بشكل افضل من أن يكون كل الحمل على راوتر واحد بهذه الطريق ستكون الشبكة تعمل بشكل افضل .
- **ملاحظة مهم جداً :** يجب أن نعرف أن لو قمنا بعمل في الشبكة الواحدة اكثر من راوتر رائيسي بمعنى **DR** سيحدث عدة مشاكل لأنه ستقوم جميع الراوتر بإرسال التحديثات و البيانات و هذا ينتج عنه مشاكل كثير في داخل الشبكة لهذا السبب يتم اختيار راوتر واحد رائيسي و الآخر احتياطي و الباقية تعمل بشكل عادي من غير مشاكل بهذا الشكل تصبح الشبكة تعمل بشكل صحيح .



- بروتوكول الـ **OSPF** يختلف عن بروتوكول الـ **RIP** و بروتوكول الـ **EIGRP** في بعض الميزات المختلفة مثل الـ **Subnet Mask** لا يكتب كما يكتب في بروتوكول الـ **RIP** بل يكتب بشكل معكوس و تسمى هذه الحالة **Wildcard Mask** هذا ما يعتمد عليه بروتوكول الـ **OSPF** , و يوجد رقم العملية التي يعمل فيها **Process id** رقم العملية هذا يقوم بتميز عملية البروتوكول مثل لو قمنا بتفعيل بروتوكول الـ **OSPF** على راوتر واحد و نريد أن نقوم بعمل تميز لهذا البروتوكول ليتكمن من تميز كل العملية على شكل مختلف عن الآخر نقوم بوضع رقم عملية جديد للبروتوكول **Process id** و هذه الميزات التي تختلف عن البروتوكولات الآخر .

- الحد الاقصى الذي يدعهم الـ **Process id** **يبدا من 1 إلى 65,535**

- الأن نريد توضيح شكل الـ **Subnet Mask** و **Wildcard Mask** لنتكن من معرفتهم :
  - **Subnet Mask** : **يكتب بهذا الشكل 255.255.255.0**
  - **Wildcard Mask** : **يكتب بهذا الشكل 0.0.0.255**

- **إعدادات بروتوكول OSPF Configuration** :

Router > **enable**

Router # **config t**

Router (config) # **router ospf 1** رقم واحد هذا هو رقم الـ **Process id**

Router (config-router) # **network 10.0.0.0 0.0.0.255 area 0**

Router (config-router) # **network 15.0.0.0 0.0.0.255 area 1**

هذه الاوامر التي تختص بعرض المعلومات الخاصة في الجداول

Router # **show ip route**

هذا الأمر لعرض جدول التوجيه

Router # **show ip ospf neighbor**

هذا الأمر لعرض الراوترات المجاورة

Router # **show ip ospf database**

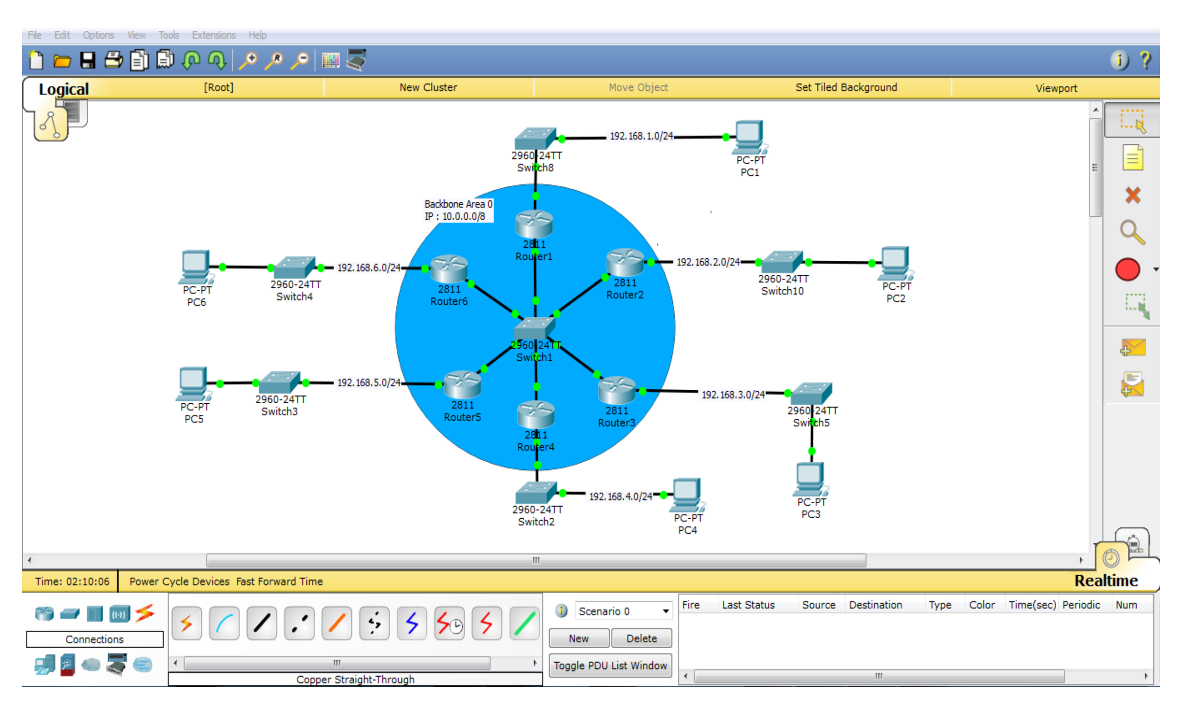
هذا الأمر لعرض قاعدة البيانات أو الطوبولوجي

OSPF Configuration, Network BMA

إعدادات بروتوكول الـ OSPF على الشبكة السريعة

- الأن سنقوم بتفعيل الـ **OSPF** على شبكة مكونة من **7** شبكات و سيتواجد نموذج للعمل عليه .
- في البداية يجب معرفة الإعدادات التي سيتم العمل عليها و معرفة الشبكات الـ **7** و معرفة الـ **Area** لنقوم بتفعيل البروتوكول على الشبكة بشكل صحيح:
  1. الشبكة الأولى ستكون بعنوان **192.168.1.0/24** .
  2. الشبكة الثانية ستكون بعنوان **192.168.2.0/24** .
  3. الشبكة الثالثة ستكون بعنوان **192.168.3.0/24** .
  4. الشبكة الرابعة ستكون بعنوان **192.168.4.0/24** .
  5. الشبكة الخامسة ستكون بعنوان **192.168.5.0/24** .
  6. الشبكة السادسة ستكون بعنوان **192.168.6.0/24** .
  7. الشبكة السابعة ستكون بعنوان **10.0.0.0/8** هذه الشبكة موجودة في **Area 0** التي ستربط ما بين الشبكات الآخر .

- الأن بعد أن تعرفنا على الشبكات و الإعدادات سنقوم بعمل إعدادات و تشغيل الإنترفيس و تركيب الاي بي على جميع الإنترفيس الموجودة على الراوترات و بعده سنقوم بتفعيل بروتوكول الـ **OSPF** لتسطيع جميع الشبكات الاتصال في بعضها البعض مثل ما في النموذج التالي المرفق اسفل وسنقوم بتعريف الشبكات في الراوترات ليتم إضافة عناوين الشبكات في جداول التوجيه ليتم الاتصال و التعرف على الشبكات بشكل صحيح و سيتم انتخاب راوتر الـ **DR** و **BDR** في شبكة **10.0.0.0/8** ليتم تعين الراوتر الرئيسي **DR** و الراوتر الاحتياطي **BDR** .



- الأن سنقوم بدخول على **R1** و عمل الإعدادات التالية :

الأن سنقوم بكتاية الاوامر التالية :

Router > **enable**

Router # **config t**

Router (config) # **interface fastethernet 0/0**

Router (config-if) # **ip address 10.0.0.1 255.0.0.0**

Router (config-if) # **no shutdown**

Router (config-if) # **exit**

Router (config) # **interface fastethernet 0/1**

Router (config-if) # **ip address 192.168.1.1 255.255.255.0**

Router (config-if) # **no shutdown**

Router (config-if) # **exit**

Router (config) # **router ospf 1**

Router (config-router) # **network 10.0.0.0 0.0.0.255 area 0**

Router (config-router) # **network 192.168.1.0 0.0.0.255 area 0**

Router (config-router) # **end**

Router # **copy running-config startup-config**

هذه إعدادات الراوتر الأول **R1** كاملة الأن سنقوم بدخول للراوتر الثاني **R2** لنقوم بعمل الإعدادات .

- الأن سنقوم بدخول على **R2** و عمل الإعدادات التالية :

الأن سنقوم بكتاية الاوامر التالية :

Router > **enable**

Router # **config t**

Router (config) # **interface fastethernet 0/0**

Router (config-if) # **ip address 10.0.0.2 255.0.0.0**

Router (config-if) # **no shutdown**

Router (config-if) # **exit**

Router (config) # **interface fastethernet 0/1**

Router (config-if) # **ip address 192.168.2.1 255.255.255.0**

Router (config-if) # **no shutdown**

Router (config-if) # **exit**

Router (config) # **router ospf 1**

Router (config-router) # **network 10.0.0.0 0.0.0.255 area 0**

Router (config-router) # **network 192.168.2.0 0.0.0.255 area 0**

Router (config-router) # **end**

Router # **copy running-config startup-config**

هذه إعدادات الراوتر الثاني **R2** كاملة الأن سنقوم بدخول للراوتر الثالث **R3** لنقوم بعمل الإعدادات .

- الأن سنقوم بدخول على **R3** و عمل الإعدادات التالية :

الأن سنقوم بكتاية الاوامر التالية :

Router > **enable**

Router # **config t**

Router (config) # **interface fastethernet 0/0**

Router (config-if) # **ip address 10.0.0.3 255.0.0.0**

Router (config-if) # **no shutdown**

Router (config-if) # **exit**

Router (config) # **interface fastethernet 0/1**

Router (config-if) # **ip address 192.168.3.1 255.255.255.0**

Router (config-if) # **no shutdown**

Router (config-if) # **exit**

Router (config) # **router ospf 1**

Router (config-router) # **network 10.0.0.0 0.0.0.255 area 0**

Router (config-router) # **network 192.168.3.0 0.0.0.255 area 0**

Router (config-router) # **end**

Router # **copy running-config startup-config**

هذه إعدادات الراوتر الثالث **R3** كاملة الأن سنقوم بدخول للراوتر الرابع **R4** لنقوم بعمل الإعدادات .

- الأن سنقوم بدخول على **R4** و عمل الإعدادات التالية :

الأن سنقوم بكتابة الاوامر التالية :

Router > **enable**

Router # **config t**

Router (config) # **interface fastethernet 0/0**

Router (config-if) # **ip address 10.0.0.4 255.0.0.0**

Router (config-if) # **no shutdown**

Router (config-if) # **exit**

Router (config) # **interface fastethernet 0/1**

Router (config-if) # **ip address 192.168.4.1 255.255.255.0**

Router (config-if) # **no shutdown**

Router (config-if) # **exit**

Router (config) # **router ospf 1**

Router (config-router) # **network 10.0.0.0 0.0.0.255 area 0**

Router (config-router) # **network 192.168.4.0 0.0.0.255 area 0**

Router (config-router) # **end**

Router # **copy running-config startup-config**

هذه إعدادات الراوتر الرابع **R4** كاملة الأن سنقوم بدخول للراوتر الخامس **R5** لنقوم بعمل الإعدادات .

- الأن سنقوم بدخول على **R5** و عمل الإعدادات التالية :

الأن سنقوم بكتابة الاوامر التالية :

Router > **enable**

Router # **config t**

Router (config) # **interface fastethernet 0/0**

Router (config-if) # **ip address 10.0.0.5 255.0.0.0**

Router (config-if) # **no shutdown**

Router (config-if) # **exit**

Router (config) # **interface fastethernet 0/1**

Router (config-if) # **ip address 192.168.5.1 255.255.255.0**

Router (config-if) # **no shutdown**

Router (config-if) # **exit**

Router (config) # **router ospf 1**

Router (config-router) # **network 10.0.0.0 0.0.0.255 area 0**

Router (config-router) # **network 192.168.5.0 0.0.0.255 area 0**

Router (config-router) # **end**

Router # **copy running-config startup-config**

هذه إعدادات الراوتر الخامس **R5** كاملة الأن سنقوم بدخول للراوتر السادس **R6** لنقوم بعمل الإعدادات .

- الأن سنقوم بدخول على **R6** و عمل الإعدادات التالية :

الأن سنقوم بكتابة الاوامر التالية :

Router > **enable**

Router # **config t**

Router (config) # **interface fastethernet 0/0**

Router (config-if) # **ip address 10.0.0.6 255.0.0.0**

Router (config-if) # **no shutdown**

Router (config-if) # **exit**

Router (config) # **interface fastethernet 0/1**

Router (config-if) # **ip address 192.168.6.1 255.255.255.0**

Router (config-if) # **no shutdown**

Router (config) # **router ospf 1**

Router (config-if) # **exit**

Router (config-router) # **network 10.0.0.0 0.0.0.255 area 0**

Router (config-router) # **network 192.168.6.0 0.0.0.255 area 0**

Router (config-router) # **end**

Router # **copy running-config startup-config**

هذه إعدادات الراوتر السادس **R6** كاملة و والاخيرة و بهذا الشكل يكون قد تم الانتهاء من برمجة جميع الراوترات و تفعيل بروتوكول الـ **OSPF** على جميع الراوترات .

- الأن بعد الانتهاء من برمجة جميع الراوترات يجب أن نتاكد هل تم إضافة جميع الشبكات في جميع الراوترات أو لا و نريد أن نقوم بعمل اختبار ما بين الشبكات كلها لنتاكد هل الشبكات تستطيع الاتصال مع بعضها البعض أو لا سنقوم بدخول على الراوتر الأول و نقوم بدخول على جدول التوجيه و نتاكد هل تم إضافة جميع الشبكات أو لا .

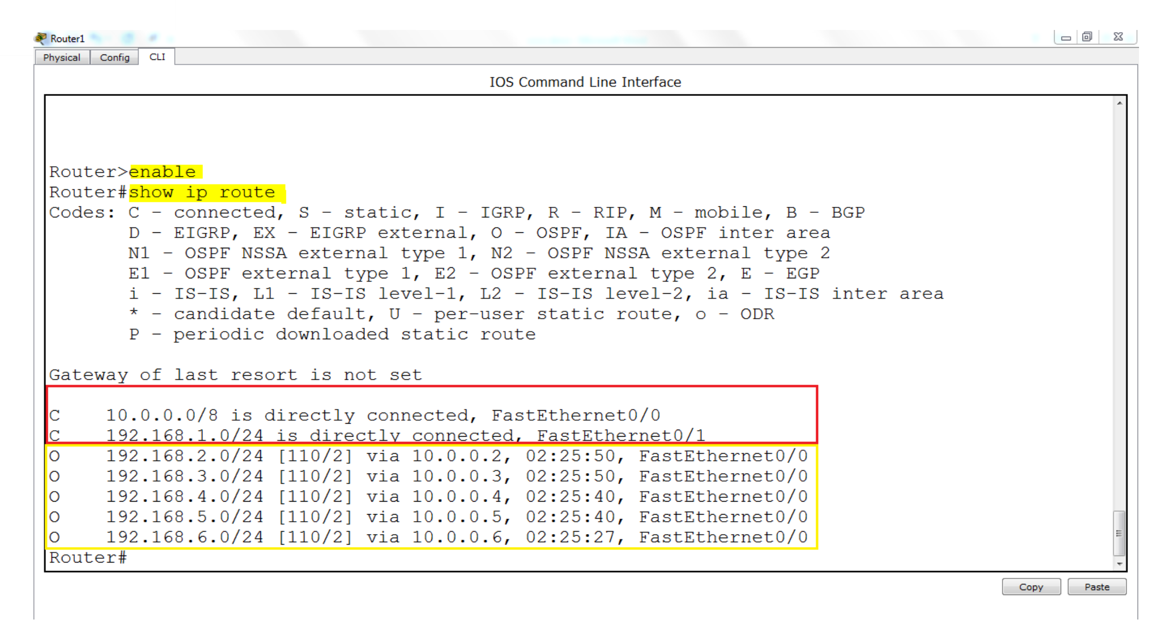
- **ملاحظة مهم جداً رمز بروتوكول الـ OSPF في جدول التوجيه O عندما نرى رمز O في جدول التوجيه يجب أن نعرف إنه تم تفعيل بروتوكول الـ OSPF .**

- الأن سنقوم بدخول على **R1** و نقوم بكتابة الأمر التالي لعرض جدول التوجيه :

Router > **enable**

Router # **show ip route**

R1



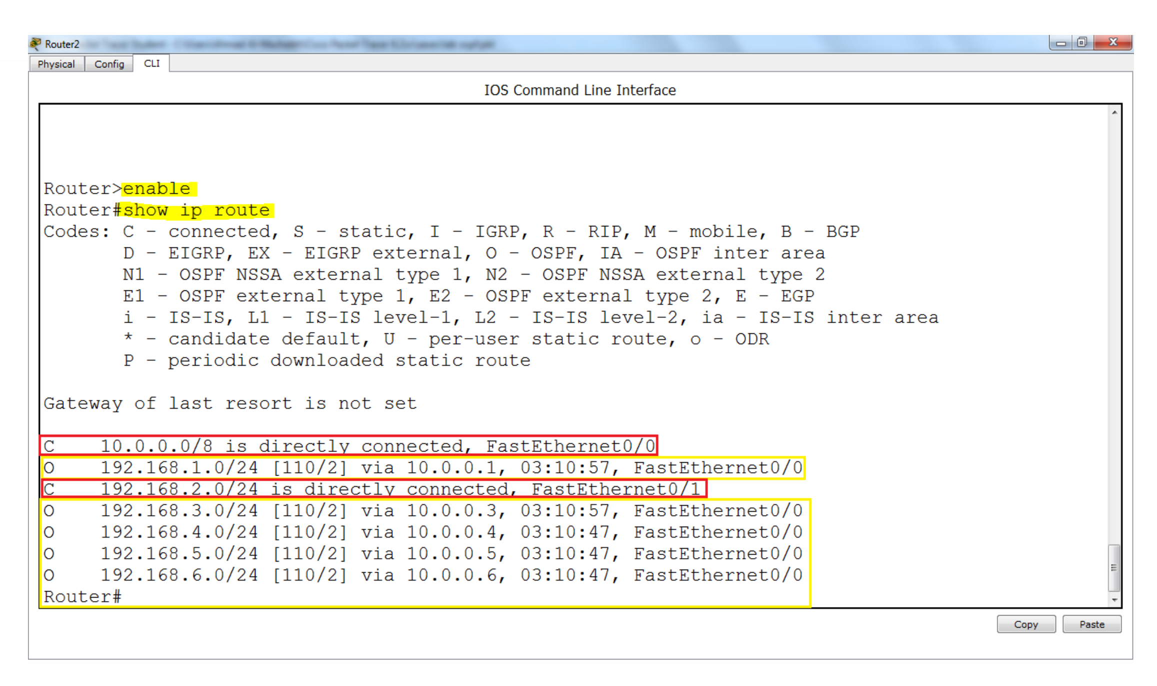
- لاحظ الأن بعد كتابة امر عرض جدول التوجيه لاحظ إنه يوجد **7** شبكات متصلة في الراوتر الأول **R1** و يستطيع الاتصال في هذه الشبكات أنظر للشبكات المحدد باللون الاصفر هذه الشبكات التي تم اضافته من خلال بروتوكول الـ **OSPF** و يجب أن نعرف أن هذه الشبكات من الطبيعي جداً إنه على راوترات تم تفعيل بروتوكول الـ **OSPF** عليهم و إذا قمنا بدخول على جميع الراوترات سنجد أن جميع الراوترات تحتوي على **7** شبكات , و بنسبه للشبكات المحددة باللون الاحمر هذه الشبكات المتصلة في الراوتر اتصال مباشر من دون بروتوكول الـ **OSPF** .

- الأن سنقوم بدخول على **R2** و نقوم بكتابة الأمر التالي لعرض جدول التوجيه :

Router > **enable**

Router # **show ip route**

R2



- لاحظ بعد كتابة امر عرض جدول التوجيه تم عرض **7** شبكات ايضاً هذا يدل على أن الراوتر الثاني **R2** قام ايضاً بتحديث جدول التوجيه لديه و قام بإضافة الشبكات .

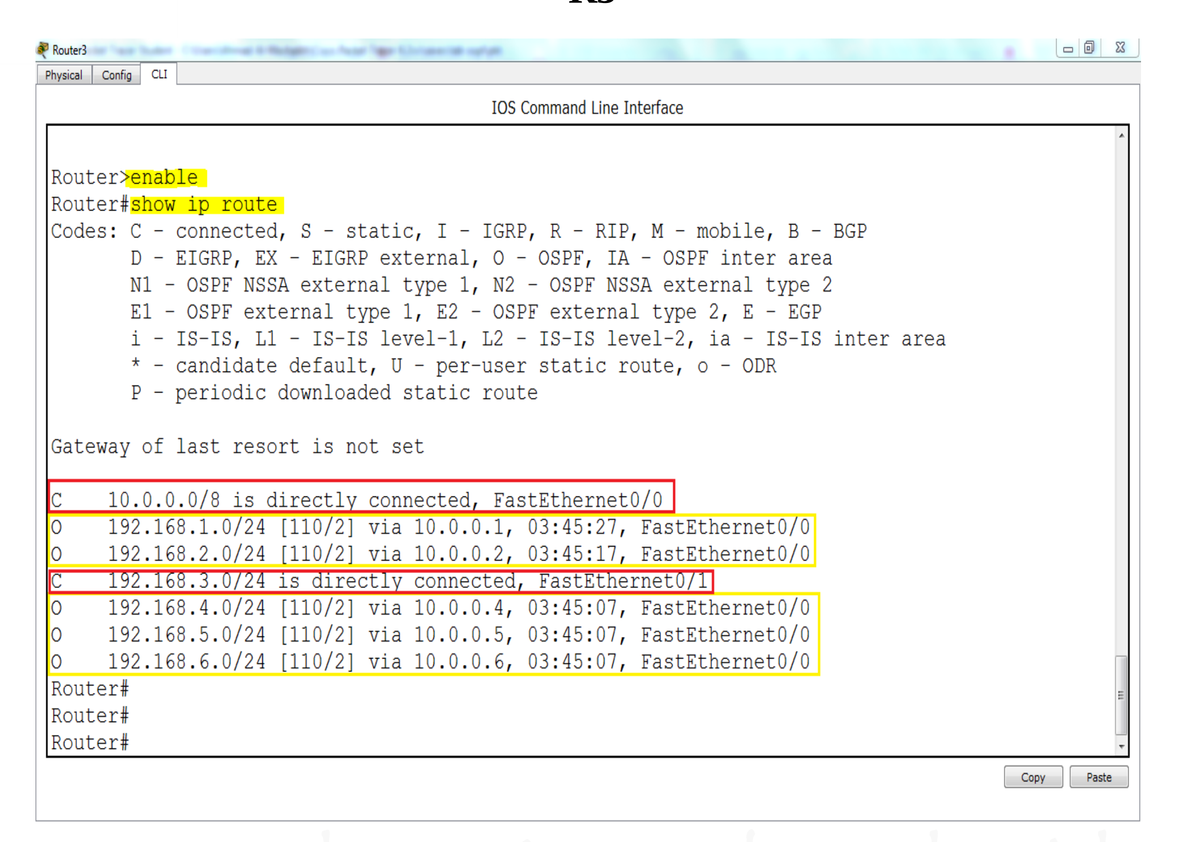
اريد أن اوضح نقطة مهم جداً أنظر للشبكات كل شبكة يتساوى على الجانب الآخر لديها رقم شبكة الـ **10.0.0.0/8** هذا عنوان شبكة الـ **Area 0** و في هذه الحالة يجب أن نعرف إنه اي شبكة من هذه الشبكة لو اردنا أن تتصل في أحد الشبكات ستقوم بتوصيل عن طريق شبكة **10.0.0.0/8** المسؤولة عن الربط ما بين الشبكات و لاحظ إنه كل شبكة تاخذ عنوان متشابه من نفس النطاق بمعنى **10.0.0.1** و **10.0.0.2** و ما بعدهم من هذه العناوين هذا لي لأنهم في نطاق واحد و في شبكة بث مباشر **BMA** في هذه الحالة يجب أن تكون جميع العناوين في نطاق واحد ليتم العمل بشكل صحيح .

- الأن سنكمل عملية عرض جداول التوجيه في الراوترات التالية **R3** و **R4** و **R5** و **R6** لنرى هل تم إضافة جميع الشبكات أو لا سنقوم بدخول عليهم واحد واحد و نقوم بكتابة الأمر التالي :

Router > **enable**

Router # **show ip route**

R3

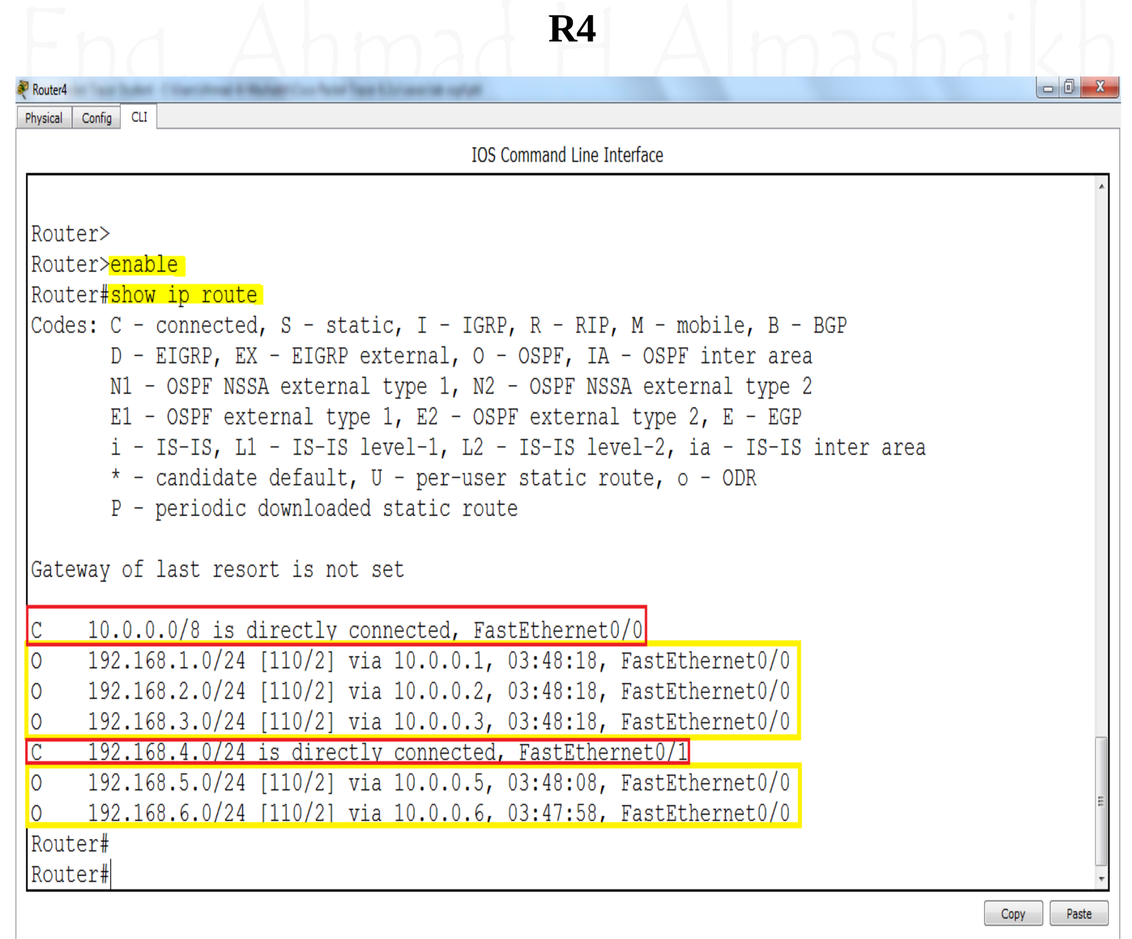


```
Router>enable
Router#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

C    10.0.0.0/8 is directly connected, FastEthernet0/0
O    192.168.1.0/24 [110/2] via 10.0.0.1, 03:45:27, FastEthernet0/0
O    192.168.2.0/24 [110/2] via 10.0.0.2, 03:45:17, FastEthernet0/0
C    192.168.3.0/24 is directly connected, FastEthernet0/1
O    192.168.4.0/24 [110/2] via 10.0.0.4, 03:45:07, FastEthernet0/0
O    192.168.5.0/24 [110/2] via 10.0.0.5, 03:45:07, FastEthernet0/0
O    192.168.6.0/24 [110/2] via 10.0.0.6, 03:45:07, FastEthernet0/0
Router#
Router#
Router#
```

R4

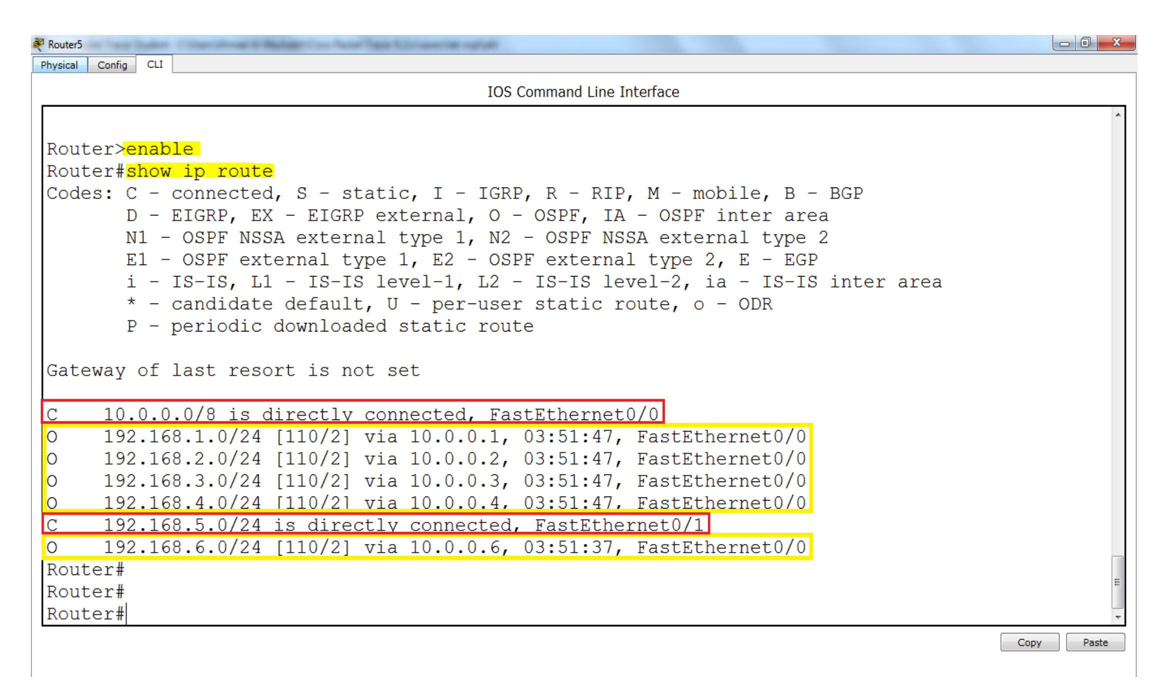


```
Router>
Router>enable
Router#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

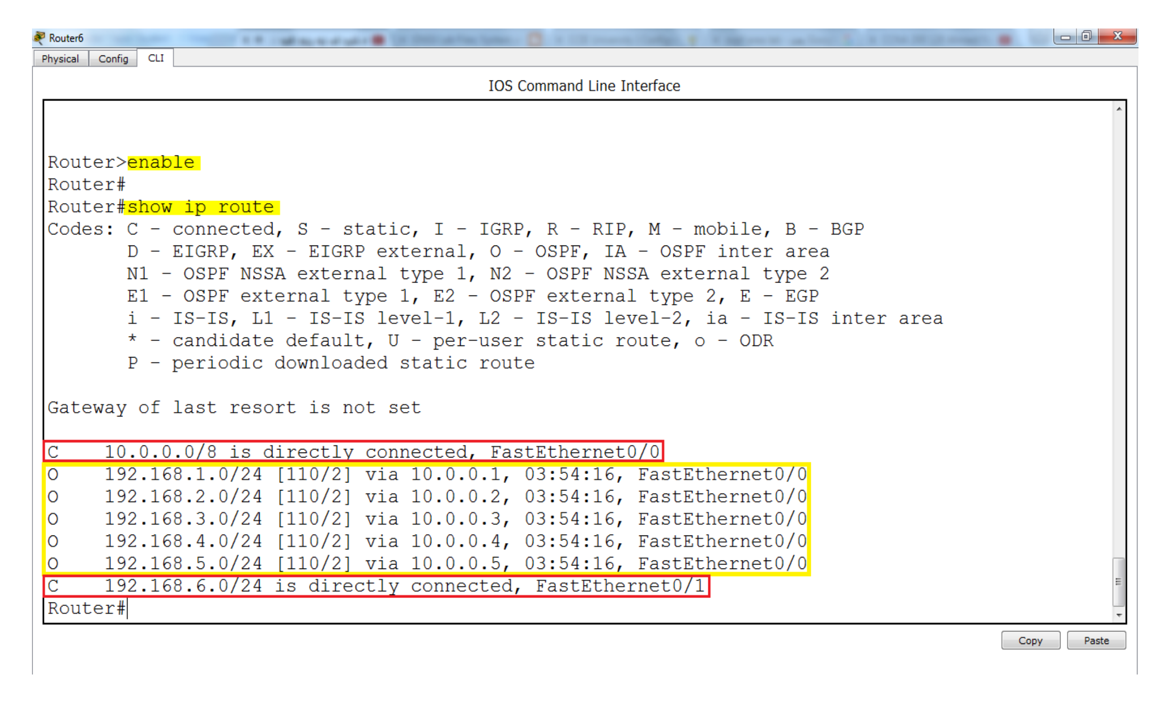
Gateway of last resort is not set

C    10.0.0.0/8 is directly connected, FastEthernet0/0
O    192.168.1.0/24 [110/2] via 10.0.0.1, 03:48:18, FastEthernet0/0
O    192.168.2.0/24 [110/2] via 10.0.0.2, 03:48:18, FastEthernet0/0
O    192.168.3.0/24 [110/2] via 10.0.0.3, 03:48:18, FastEthernet0/0
C    192.168.4.0/24 is directly connected, FastEthernet0/1
O    192.168.5.0/24 [110/2] via 10.0.0.5, 03:48:08, FastEthernet0/0
O    192.168.6.0/24 [110/2] via 10.0.0.6, 03:47:58, FastEthernet0/0
Router#
Router#
```

R5



R6



- الأن بعد أن قمنا بعرض جداول التوجيه لجميع الراوترات نرى إنه يوجد في كل راوتر 7 شبكات و جميعهم متصلين مع بعضهما البعض عن طريق شبكة الـ **Backbond** **Area 0** التي له عنوان **10.0.0.0/8** و بهذا الشكل يتم الاتصال ما بين جميع الشبكات.

- الأن بعد أن قمنا بتفقد جدول التوجيه في جميع الراوترات نريد أن نعرف من الراوتر الرئيسي **DR** و الراوتر الاحتياطي **BDR** سنقوم بدخول على أول راوتر تم تفعيل بروتوكول الـ **OSPF** عليه و نقوم بكتابة الأمر التالي :

- في البداية قمنا بتفعيل بروتوكول الـ **OSPF** على الراوتر الأول **R1** سنقوم بدخول عليه و كتابة الأمر التالي :

Router # **show ip ospf neighbor**

R1

```
Router#show ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
192.168.2.1       1   FULL/DROTHER    00:00:36    10.0.0.2        FastEthernet0/0
192.168.3.1       1   FULL/BDR        00:00:39    10.0.0.3        FastEthernet0/0
192.168.4.1       1   FULL/DROTHER    00:00:35    10.0.0.4        FastEthernet0/0
192.168.5.1       1   FULL/DROTHER    00:00:38    10.0.0.5        FastEthernet0/0
192.168.6.1       1   FULL/DROTHER    00:00:31    10.0.0.6        FastEthernet0/0
```

- بعد أن قمنا بدخول على الراوتر الأول **R1** و قمنا بعرض جدول الجيران لنعرف من هو الراوتر الرئيسي ولكن في هذا الراوتر لم يعرض من هو الراوتر الرئيسي **DR** و في هذه الحالة يجب أن نعرف إنه هذا هو الراوتر الرئيسي و لنتاكد من إنه الراوتر الرئيسي **DR** سنقوم بدخول على راوتر اخرى مثل الراوتر الثاني **R2** لنتاكد من هو الراوتر الرئيسي **DR** ولكن في هذه الحالة لاحظ إنه تم عرض الراوتر الاحتياطي **BDR** و ياخذ عنوان الشبكة **192.168.3.1** في هذه الحالة قمنا بمعرفة من هو الراوتر الاحتياطي .

- الأن لنتاكد من الراوتر الرئيسي سنقوم بدخول على الراوتر الثاني **R2** و نقوم بكتابة الأمر التالي.

Router # **show ip ospf interface**

R2

```
Router#show ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
192.168.3.1       1   FULL/BDR        00:00:36    10.0.0.3        FastEthernet0/0
192.168.1.1       1   FULL/DR         00:00:36    10.0.0.1        FastEthernet0/0
192.168.4.1       1   2WAY/DROTHER    00:00:32    10.0.0.4        FastEthernet0/0
192.168.5.1       1   2WAY/DROTHER    00:00:36    10.0.0.5        FastEthernet0/0
192.168.6.1       1   2WAY/DROTHER    00:00:38    10.0.0.6        FastEthernet0/0
```

- الأن لاحظ إنه تم عرض جدول الجيران و تم عرض الراوترات و حالة الراوترات لاحظ الأن إنه تم معرفة الراوتر الرئيسي **DR** ياخذ عنوان الشبكة **192.168.1.1** و نفهم من هذا إنه الراوتر الأول **R1** هو الراوتر الرئيسي و بهذا الشكل نكون قد تعرفنا على حالة الراوتر في الشبكة .
- فيه هذا الدرس تم العمل على شبكة الـ **BMA** الشبكة السريعة التي تعمل في نطاق واحد الأن نريد أن نقوم بعمل شبكة **Point-to-Point** شبكة النقطة للنقطة لنتعرف كيفية العمل عليها و مفهومها .

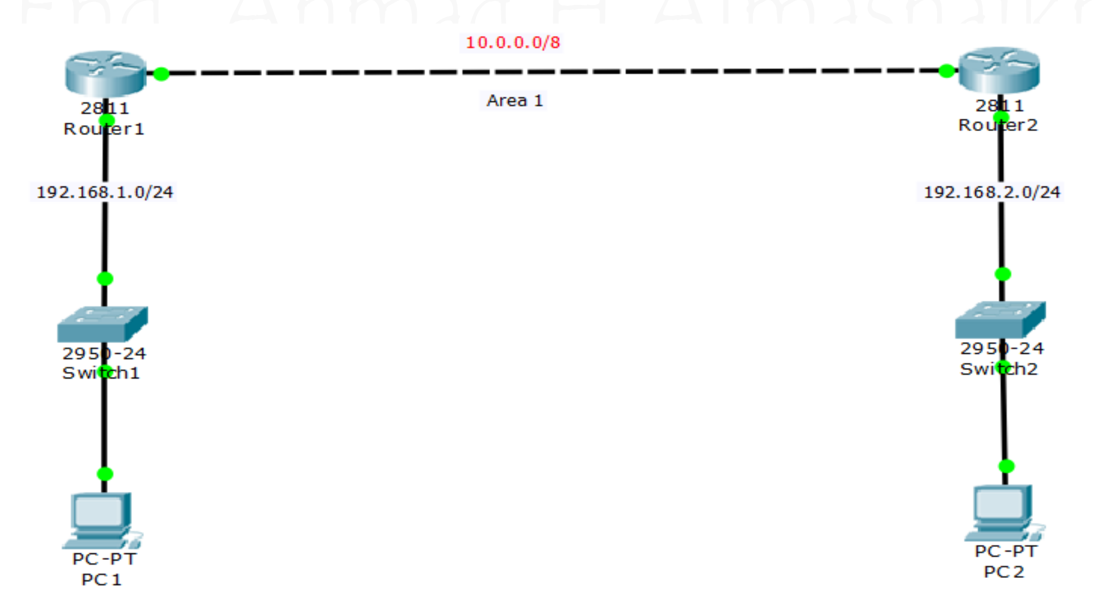
OSPF Configuration, Network Point-to-Point

إعدادات بروتوكول الـ OSPF على شبكة النقطة للنقطة

- **الأن سنقوم بتفعيل الـ OSPF على شبكة مكونة من 3 شبكات و سيتواجد نموذج للعمل عليه .**
- **في البداية يجب معرفة الإعدادات التي سيتم العمل عليها و معرفة الشبكات الـ 3 و معرفة الـ Area لنقوم بتفعيل البروتوكول على الشبكة بشكل صحيح:**

١. الشبكة الأولى ستكون بعنوان **192.168.1.0/24** .
٢. الشبكة الثانية ستكون بعنوان **192.168.2.0/24** .
٣. الشبكة الثالثة ستكون بعنوان **150.0.0.0/8** .

- الأن بعد أن تعرفنا على الشبكات و الإعدادات سنقوم بعمل إعدادات و تشغيل الإنترفيس و تركيب الاي بي على جميع الإنترفيس الموجودة على الراوترات و بعده سنقوم بتفعيل بروتوكول الـ **OSPF** لتسطيع جميع الشبكات الاتصال مع بعضها البعض مثل ما في النموذج التالي المرفق اسفل وسنقوم بتعريف الشبكات في الراوترات ليتم إضافة عناوين الشبكات في جداول التوجيه ليتم الاتصال و التعرف على الشبكات بشكل صحيح و سيتم انتخاب راوتر الـ **DR** و **BDR** في شبكة **10.0.0.0/8** ليتم تعين الراوتر الرئيسي **DR** و الراوتر الاحتياطي **BDR** .



- الأن سنقوم بدخول على الراوترات و نقوم بعمل برمجة لكل راوتر سنقوم بدخول على الراوتر الأول **R1** و نقوم بتشغيل الإنترفيس و تركيب الاي بي عليه و بعدها نقوم بتفعيل البروتوكول الـ **OSPF** عليه و بعد الانتهاء سننتقل للراوتر الثاني و نقوم بنفس الإعدادات و بعد الانتهاء سنقوم بعمل اختبار للشبكة لنرى هل تعمل بشكل صحيح أو يوجد اخطاء .

- الأن سنقوم بدخول على **R1** و عمل الإعدادات التالية :

الأن سنقوم بكتابة الاوامر التالية :

Router > **enable**

Router # **config t**

Router (config) # **interface fastethernet 0/0**

Router (config-if) # **ip address 10.0.0.1 255.0.0.0**

Router (config-if) # **no shutdown**

Router (config-if) # **exit**

Router (config) # **interface fastethernet 0/1**

Router (config-if) # **ip address 192.168.1.1 255.255.255.0**

Router (config-if) # **no shutdown**

Router (config-if) # **exit**

Router (config) # **router ospf 1**

Router (config-router) # **network 10.0.0.0 0.0.0.255 area 1**

Router (config-router) # **network 192.168.1.0 0.0.0.255 area 1**

Router (config-router) # **end**

Router # **copy running-config startup-config**

هذه إعدادات الراوتر الأول **R1** كاملة الأن سنقوم بدخول للراوتر الثاني **R2** لنقوم بعمل الإعدادات .

- الأن سنقوم بدخول على **R2** و عمل الإعدادات التالية :

الأن سنقوم بكتابة الاوامر التالية :

Router > **enable**

Router # **config t**

Router (config) # **interface fastethernet 0/0**

Router (config-if) # **ip address 10.0.0.2 255.0.0.0**

Router (config-if) # **no shutdown**

Router (config-if) # **exit**

Router (config) # **interface fastethernet 0/1**

Router (config-if) # **ip address 192.168.2.1 255.255.255.0**

Router (config-if) # **no shutdown**

Router (config-if) # **exit**

Router (config) # **router ospf 1**

Router (config-router) # **network 10.0.0.0 0.0.0.255 area 1**

Router (config-router) # **network 192.168.2.0 0.0.0.255 area 1**

Router (config-router) # **end**

Router # **copy running-config startup-config**

هذه إعدادات الراوتر الأول **R2** كاملة الأن سنقوم بهذه الطريقة و الإعدادات نكون قد تم الانتهاء من جميع الإعدادات بشكل كامل و نريد أن نقوم بعمل اختبار للشبكة نتابع التالي .

- سنقوم بدخول على الراوتر الأول **R1** و نقوم بكتابة الأمر **Ping** لنتصل في الراوتر الثاني **R2** إذا تم الرد بعلامة **!!!!!** بهذا الشكل هذا يدل على إنه الشبكة تعمل بشكل صحيح اما إذا تم الرد بهذا الشكل ..... هذا يعني إنه يوجد خطاء في الشبكة و لا تسطيع الاتصال في الراوتر الثاني أنظر ا الصورة التالية من داخل الراوتر الأول **R1**..........

```
R1#ping 10.0.0.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.0.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/1 ms

R1#
```

- لاحظ إنه تم الرد بعلامة **!!!!!** من الراوتر الثاني **R2** بهذه الطريقة نتاكد أن الشبكة تعمل بشكل صحيح و من دون اية مشاكل .
- الأن نريد معرفة من هو الراوتر الرئيسي **DR** في الشبكة و من هو الراوتر الاحتياطي **BDR** .

R1

```
Neighbor ID     Pri   State           Dead Time   Address         Interface
192.168.2.1       1   FULL/DR         00:00:35    10.0.0.2        FastEthernet0/0
R1#
```

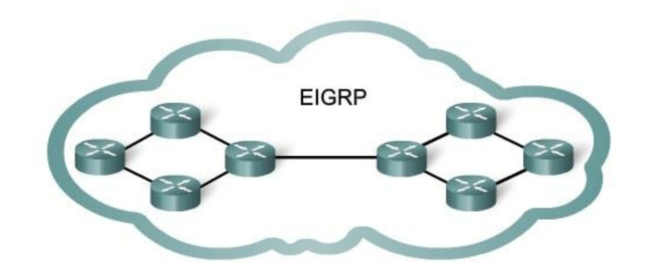
R2

```
Neighbor ID     Pri   State           Dead Time   Address         Interface
192.168.1.1       1   FULL/BDR        00:00:34    10.0.0.1        FastEthernet0/0
R2#
```

EIGRP

Enhanced Interior Gateway Routing Protocol

بروتوكول توجيه البوابة الداخلية المحسن



- بروتوكول خاص في شركة سيسكو و يتم تطويره و و برمجته من قبل شركة سيسكو نفسها **Cisco Routing Protocol**.
- بروتوكول الـ **EIGRP** هو مطور من بروتوكول قديم **Enhance to IGRP** كان يعمل قبل أن يتم تطوير الـ **EIGRP** و الأن يعتمد العمل على بروتوكول الـ **EIGRP**.
- يعتبر بروتوكول الـ **EIGRP** هيجن لي لأنه يحتوي على خوارزمية أقصر مسار و خوارزمية اسرع مسار بمعنى إنه ينتمي إلي عائلة الـ **Link Status Protocol** و عائلة **Distance Vector**.
- يدعم عدد القفزات لحد **224** **Netxt Hop Count** في المسار الذي يعمل فيه بروتوكول الـ **EIGRP** .
- يعمل بنظام الـ **Dual** في عملية اختيار المسار الافضل من مجموعة مسارات موجودة في الشبكة .
- يعمل باستخدام تحديثان التحديث الفوري و التحديث الدوري و كل منهم له وظيفة .
- التحديث الفوري يقوم بإرسال رسالة عند حدوث تغير أو تعديل في الجداول **Triggered Update**.
- التحديث الدوري **Periodic Update** هو التحديث المنظم في البروتوكول بمعنى إنه يقوم كل وقت معين بإرسال رسال دورية لستكشاف الجيران هل الراوترات تعمل أو هل الراوترات متوقفة عن العمل أو ما شابه .
- يعمل بعنوان البث المتعدد الخاص فيه **224.0.0.10**.
- يعمل على ثلاث جداول مثل بروتوكول الـ **OSPF** ولكن هنا تختلف الاسماء في بروتوكول الـ **EIGRP** سأقوم بذكرها و شرحها .
- يعمل على تقسيم الراوترات على عدة مناطق تسمى **Autonomous System = AS** على مختلف بروتوكول الـ **OSPF** الذي يقسم المنطاق على **Area**.
- قيمة المسافة الإدارية لبروتوكول الـ **EIGRP 90 Administrative distance**
- بروتوكول الـ **EIGRP** هو البروتوكول الوحيد الذي يعمل على مسار رائيسي و مسار احتياطي فقط في حال تم ايقاف المسار الرئيسي سيتم التحويل على المسار الاحتياطي بشكل تلقائي على عكس البروتوكولات الآخر .

- يعمل على توزيع الترافيك ما بين المسارات لتوزيع الحمل عن المسار و تقليل الضغط.
- يدعم كلمات المرور و تشفيرها .
- يدعم تشفير الـ **MD5**.
- يعمل مع بروتوكولات **IP, Apple Talk , IPx**.
- يعمل بشكل دوري على مراقبة المسارات و التغيرات التي تحدث و في حال تم وقوع مسار أو عطل ستتم عملية التحويل بسرعة .
- بروتوكول الـ **EIGRP** لا يعمل مع بروتوكولات الـ **UDP** و **TCP** .
- يعمل في الطبقة الثالثة و هي طبقة الشبكة **Network Layer 3**.
- يدعم خاصية الـ **Summarization** بشكل اتوماتيكي .
- يدعم خاصية الـ **CIDR** و **VLSM** .
- يدعم تقسيم الشبكة **Classless**.

جداول بروتوكول الـ EIGRP

EIGRP Table

١- جدول الجيران Neighbor Tabe

هذا الجدول الذي يتم فيه ادراج الراوترات المجاورة لديها في الشبكة المرتبطة فيه بشكل مباشرة و التي تم تفعيل بروتوكول الـ **EIGRP** عليها لتتمكن من الاتصال في بعضها البعض و ايضاً يتم ادراج مسارات القفزات و الإنترفيس و العمل تحت إشراف بروتوكول الـ **EIGRP** .

الأمر الذي يقوم بعرض هذا الجدول هو الأمر التالي :

Router # **show ip ospf neighbors**

٢- جدول الطوبولوجي Topology Table

هذا الجدول الذي يحتوي علىمخطة الشبكة كله بمعنى إنه يقوم بتسجيل جميع الطوبولوجي الخاص في الجيران و يحتوي ايضاً على النظام المتريك Metric و اسماء الراوترات .

الأمر الذي يقوم بعرض هذا الجدول هو الأمر التالي :

Router # **show ip ospf topology**

٣- جدول التوجيه Routing Table OR Global Routing Table

هذا جدول التوجيه يتم تسجيل فيه تسجيل جميع المسارات و العناوين المجاورة للشبكة و عندما يريد أحد الجيران شبكة معينة يقوم بنظر على جدول التوجيه من حيث يختار افضل مسار للوصول للشبكة المطلوبة .

الأمر الذي يقوم بعرض هذا الجدول هو الأمر التالي :

Router # **show ip route**

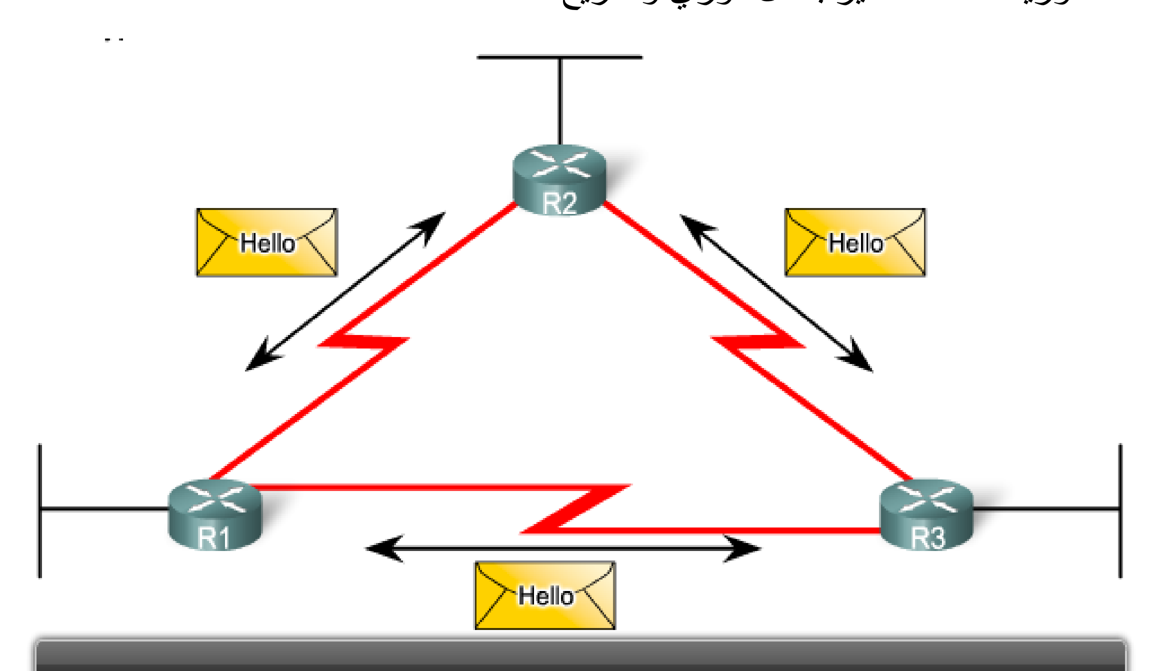
أنواع حزم البيانات الخاصة في بروتوكول التوجيه الـ EIGRP

EIGRP Packet Types

Hello Packets, Update Packet, Query Packet, Relpy Packet, ACK Packet

- حزم البيانات يتم استخدمها فيما بين الراوترات التي تم تفعيل بروتوكول الـ **EIGRP** عليها لتتمكن من بناء و صيانة الجداول الثلاثة الموجودة في كل راوتر.
- تتكون حزم البيانات من **5** أنواع سأقوم بذكرها و شرح كل واحدة بشكل منفصل عن الأخرى.

١- **رسالة الترحيب Hello Packet:** هي عبارة عن رسالة ترحيب يتم إرسالها في وقت معين و يستطيع مهندس الشبكة تحديد هذا الوقت الخاص في الرسالة و يوجد وقت تلقائي لهذا الرسالة سأقوم بذكرها في ما بعد وظيفة هذه الرسالة تكون بشكل دوري أو فوري مثل عندما يحدث تغير أو تعديل في أحد الراوترات الموجودة في الشبكة سيتم إرسال هذه الرسالة بشكل فوري بمعنى إنه حدث تغير أو تعديل يجب أن تبعث هذه الرسالة لنرى ماذا حدث هل تم حذف أو تعديل أو تغير في الشبكة هذه وظيفة هذه الرسالة تقوم بعملية استكشاف للشبكة التي تم تفعيل بروتوكول الـ **EIGRP** عليه و في حال لم يتم التعديل أو التغير أو ما شابه من هذه الاشياء سيتم إرسال هذه الرسالة بشكل دوري بمعنى كل وقت زماني محدد لتتم عملية الاستكشاف و المراقبة للشبكة بشكل دوري ولكن هذه الرسالة تكون بشكل غير موثوق بمعنى من الممكن أن يكون أحد الراوترات متوقف عن العمل و هذه الرسالة من الممكن إنه لا تقوم بكشف هذا الراوتر على عكس الرسالة الفورية تكشف التغير بشكل دوري و سريع ؟



Hello packet
- Use to discover neighbors & form adjacencies
- Unreliable so no response required from recipient

محتويات رسالة الترحيب Hello Packets : في البداية رسالة الترحيب في بروتوكول الـ **EIGRP** تتكون من **Message Format** وتحتوي في داخلها على عدة خانات مكونة في داخله معلومات يتم بناء الرسالة عليه سأقوم بذكهم و شرحهم .

- تبداء عملية التغليف بشكل مرتب و تسمى هذه العملية **Encapsulated EIGRP Message** مكونة من اربع خانات سأقوم بذكرهم :

1- Data Link Frame Header, 2- IP Packet Header, 3- EIGRP Packet Header , 4- Type / Length / Values Types.

كما في النموذج التالي

Encapsulated EIGRP Message

Data Link Frame Header	IP Packet Header	EIGRP Packet Header	Type/Length/Values Types

Data Link Frame
MAC Destination Address = Multicast: 01-00-5E-00-00-0A
MAC Source Address = Address of sending interface

IP Packet
IP Source Address = Address of sending interface
IP Destination Address = Multicast: 224.0.0.10
Protocol field = 88 for EIGRP

EIGRP Packet Header
Opcode for EIGRP packet type
AS Number

TLV Types
Some types include:
0x0001 EIGRP Parameters
0x0102 IP Internal Routes
0x0103 IP External Routes

- الأن سأقوم بشرح كل واحدة من هذه الخانات الاربعة بشكل منفرد عن الآخر لنفهم كل خانة ما هي وظيفتها و على ماذا تحتوي من المعلومات .

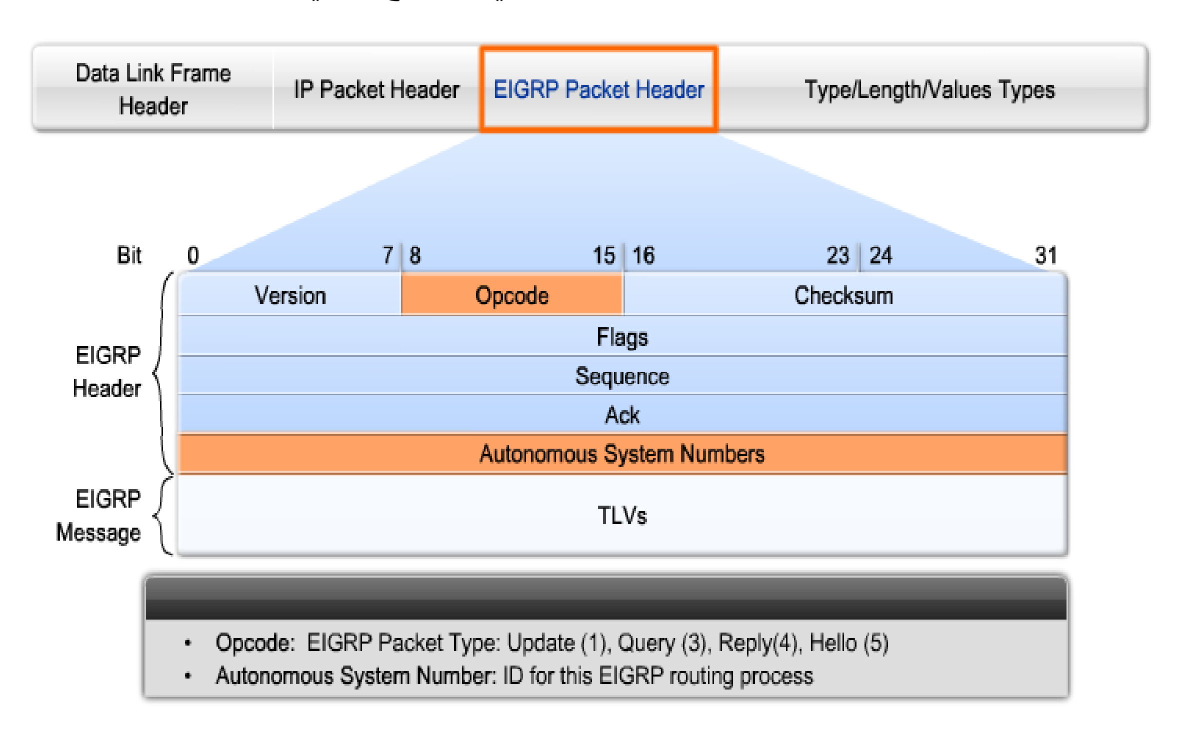
١- **Data Link Frame Header:** هذه الخانة المسؤولة عن الإطار الذي يتم فيه تخزين و تركيب عناوين الماك ادرس لجهاز المرسل و المستقبل **MAC Destination Address** و **MAC Source Address** لتتم عملية الإرسال مابين الأجهزة.

٢- **IP Packet Header :** هذه الخانة المسؤولة عن الـ **IP Packet** والتي يتم فيها وضع عناوين الاي بي الخاصة بجهاز المرسل و جهاز المستقبل **IP Source Address** و **IP Destination Address** و تحتوي ايضاً على حقل بروتوكول الـ **EIGRP**.

٣- **EIGRP Packet Header :** هذه الخانة المسؤولة عن رمز أنواع الحزمة و رقم المنطقة **AS** و سأقوم بشرح تفصيلي لهذه الخانة لي لأنه تحتوي على **Header** مكون من عدة خانات و طول هذا الـ **Header 31 Bit** و يحتوي في داخله عدة خانات سأقوم بذكر هذه الخانات و شرحها .

٤- **Type / Length / Values Types:** هذه الخانة تحتوي على البيانات الخاصة في حقول الـ **EIGRP Message** المسؤولة عن الاتصال و تحديد النوع و الطول و القيمة و الحقل و هي التي تشمل كل الحقول الخاصة في الـ **Message Format**.

EIGRP Packet Header : يتكون هذا الحقل من عدة خانات و يتكون في داخل **Header** طول هذا الـ **Header 31 bit** كما في النموذج التالي:



- **سأقوم بشرح كل هذه الخانات الموجودة في داخل الـ Header لنتعرف على كل واحدة منهم ماذا تفعل و ما هي وظيفة كل واحدة منهم .**

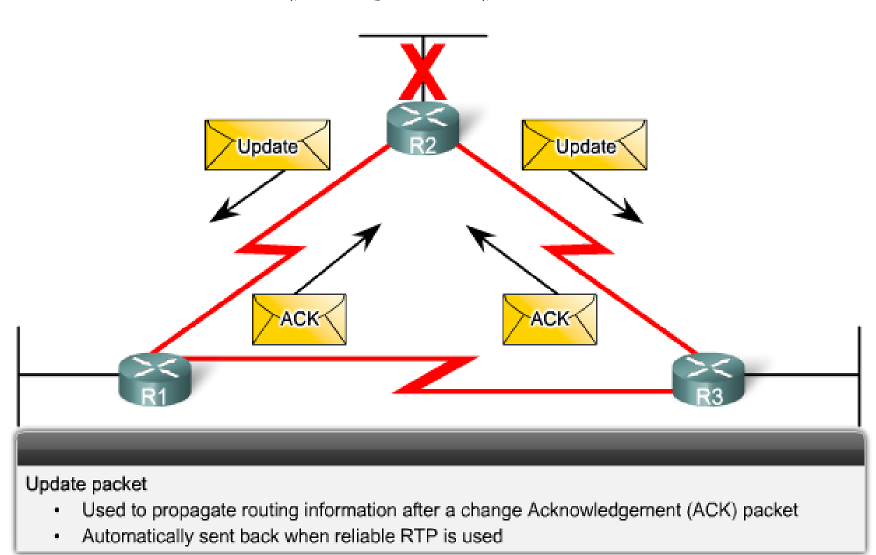
1- Version
2- Opcode
- **Flags**
- **Sequence**
- **Ack**
- **Autonomous System Numbers**
3- Check sum
4- TLVs / EIGRP Message

- **هذه هي المكونات الأن سأقوم بشرحهم و معرفة كل منهم ماذا تحتوى :**

- **Version:** هذه الخانة التي يتم فيها تخزين اصدار البروتوكول و موصفات البروتوكول.
- **Opcode :** هذه الخانة التي تحتوي على عدة خانات مثل تبداء في تكوين البيانات و تقوم بعمل الإعدادات وإضافة المعلومات و بعده تقوم بنقلها للخانة الآخر و سنقوم بشرح هذه الخانات الموجودة في داخل هذه الخانة .
- **Flags :** هذه الخانة المسؤولة عن أعلام بداية تكوين الحزمة في الـ **Header** و تبداء في عملية التكوين و النزول للخانة الثانية .
- **Sequence :** هذه الخانة المسؤولة عن تسلسل الحزم في الـ **Header**.
- **Ack :** هذه الخانة المسؤولة عن إشعار إستلام الحزمة و بعده سيتم النزول للخانة الآخر **AS** ليتم التحديد لـ اية **AS** سترسل هذه الحزمة .
- **Autonomous System Numbers:** هذه الخانة المسؤولة عن تحديد رقم المنطقة المراد الإرسال اليها الحزمة.
- **Check sum :** هذه الخانة المسؤولة عن مراقبة اية اخطاء و وظيفة هذه الخانة انها تقوم بعملية استكشاف للحزمة قبل أن ترسل للجهاز المطلوب.
- **TLVs :** هذه الخانة كما شرحنا من قبل هي المسؤولة عن أنواع الاتصال بمعنى هي المسؤولة عن عملية إرسال الحزم و يوجد اكثر من نوع لعملية الاتصال و الإرسال .

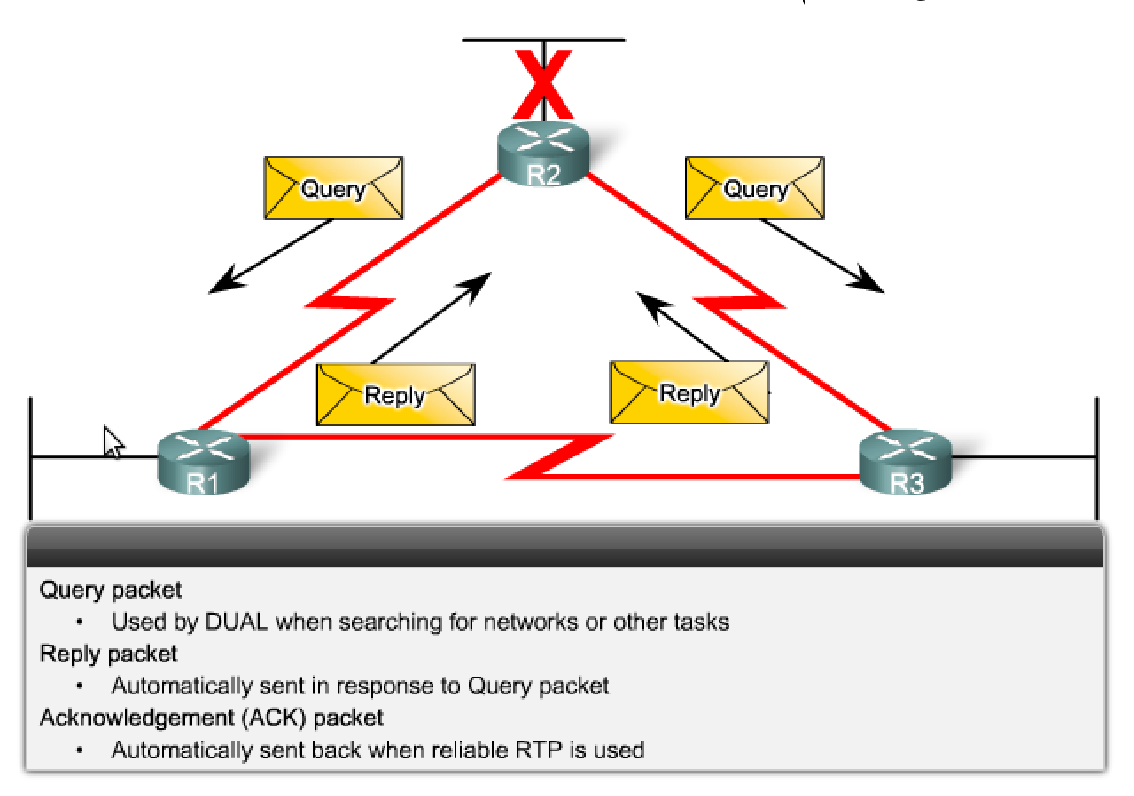
٢- **Update Packet :** هذه الحزمة المسؤولة عن عملية التحديثات مثل عندما نقوم بإضافة شبكة جديدة أو حذف شبكة أو التعديل في البيانات أو ما شابه سنقوم بعملية إرسالة حزمة في المتغيرات التي تم تغيرها ليتم التحديث في جميع الراوترات التي تعمل ببروتوكل الـ **EIGRP** لتبقى جميع الراوترات لديها جميع البيانات و المعلومات و المسارات و التحديثات و ترسل فقط هذه الحزمة للراوتر الذي تم إضافة في الشبكة لياخذ التحديثات و هذه الرسالة فقط يتم إرساله عندما يحتاج أحد الراوترات تغير أو تحديث ولا يتم إرساله بشكل متكرر بمعنى إنه ترسل بشكل فوري .

كما في النموذج التالي



- و عندما يستلم الراوتر المطلوب التحديث سيقوم برد على الراوتر الذي قام بإرسال التحديثات برسالة تاكيد **ACK** على إنه تم استلام التحديثات بشكل صحيح و تم التعديل و التحديث و بهذا الشكل يكون الراوتر قد حصل على جميع التحديثات التي تم التعديل فيها أو التغير فيه .

٣- **Query Packet :** هذه الرسالة أو الحزمة مسؤالة عن عملية إرسال الحزمة في عدة مسارات مثل يوجد لدينا اكثر من مسار و نستطيع إرسال الحزمة على اكثر من مسار و هذا يعني لو حد مشكلة ما في أحد المسارات تستطيع إرسال إلى مسار اخرى و هذا يدل على إنه تستخدم خوارزمية الـ **Dual** وبعد الإرسال ترد علينا برسالة تاكيد **ACK** من الطرفين على الاستلام .



٤- **Relpy Packet :** هذه الرسالة ترسل ما بعد وظيفة الـ **Query Packet** .

٥- **ACK Packet :** هذه الرسالة الاخيرة التي بعد أن تقوم جميع الراوترات باسلام التحديثات و التغيرات و التعديلات سيتم إرسال رسالة تاكيد إنه تم التحديث بشكل صحيح.



- **توقيت رسالة الترحيب في بروتوكول الـ EIGRP :**
- **من الطبيعي إنه يوجد توقيت لرسالة الترحيب في كل وقت معين و يختلف الوقت من شبكة لـ شبكة اخرى سنقوم بتعرف على التوقيت في الشبكة .**

توقيت رسالة الترحيب **Hello Packet** في الشبكة السريعة كل **5** ثواني و في حال عدم وجود الراوتر سيبقى ينتظر **15** ثانية بعدها سيعتبر الراوتر غير موجود في الشبكة .

هذا التوقيت في الشبكة السريعة BMA= Broadcast Multiaccess Network / Point – to -Point

توقيت رسال الترحيب في الشبكة البعيدة و التي لا تكون في نطاق واحد مثل يربط ما بينهم **Frame Relay , MPLS** و في هذه الشبكات يكون التوقيت **60** ثانية لعملية إرسال رسالة الترحيب و إذا لم يتم الرد يبقى يرسل لوقت **180** ثانية و بعده سيعتبر الراوتر غير موجودة .

هذا التوقيت في الشبكة الـ **NBMA = Non Broadcast Multiaccess**

- الفرق بين التحديث الفوري **Triggered Update** و التحديث الدوري **Periodic Update :**

- **التحديث الفوري Triggered Update :** يحدث التحديث الفوري عند حدوث تغير في الجداول في أحد الراوترات مما ينتج عن إرسال تحديث فوري لكل الراوترات الموجودة في الشبكة ليتم التعديل في باقي الراوترات .

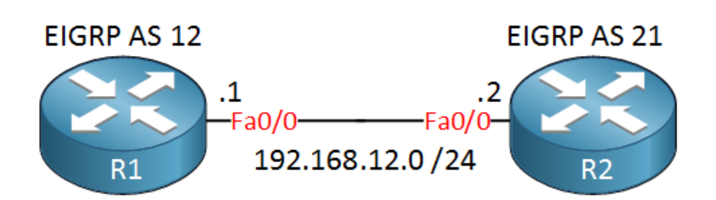
- **التحديث الدوري Periodic Update :** يحدث التحديث الدوري بشكل دوري بمعنى إنه يوجد توقيت معين يحدث فيه هذا التحديث في زمن معين يقوم بإرسال رسالة يتاكد فيها هل الراوترات تعمل هل المسارات مفعله هذا هو التحديث الدوري .

- **يقوم بإرسال رسالة الترحيب على العنوان 224.0.0.10 بشكل Multicast .**



بناء العلاقات ما بين الجيران في بروتوكول الـ EIGRP

EIGRP Neighbor Adjacencies

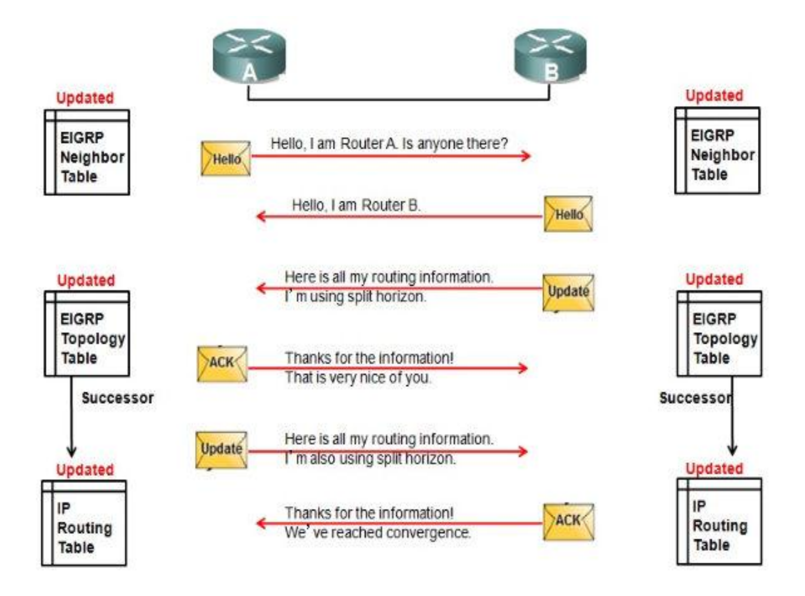


- مرحلة بناء العلاقات ما بين الجيران أو الراوترات تتم بعد 7 خطوات اساسية سأقوم بذكرها و التعرف عليها .

1- **Hello Packet** رسالة الترحيب
2- **Hello + Update** رسالة الترحيب و التحديث
3- **Ack** رسالة التاكيد على استلام الحزمة
4- **Modify Topology Table** التعديل في الجدأول
5- **Update** إرسال التحديثات التي تم التعديل عليه
6- **Ack** رسالة التاكد على استلام الحزمة
7- **Modify Topology Table** رسالة التعديل في الجدأول

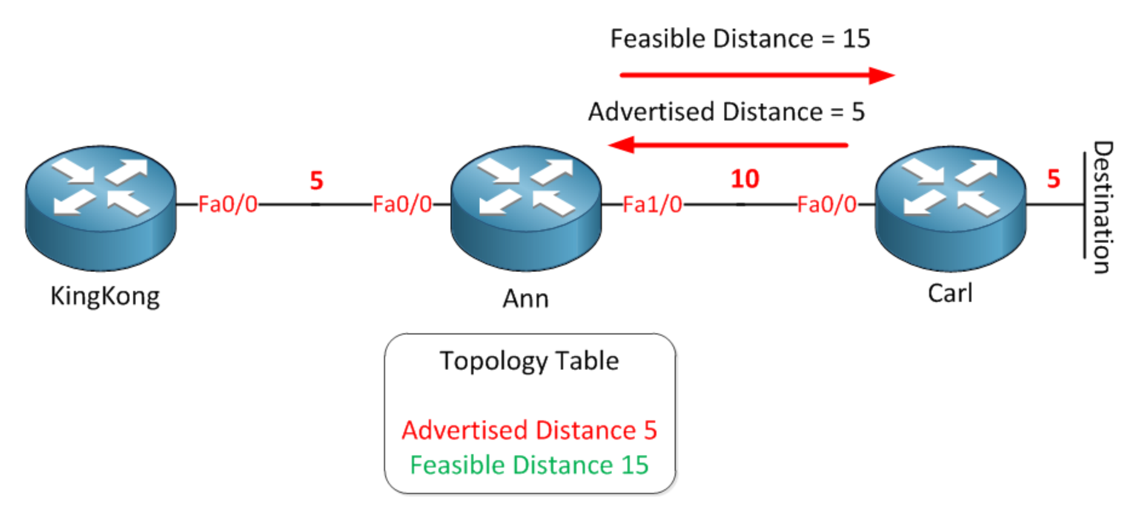
- هذه مرحلة بناء العلاقة ما بين الراوترات التي تم تفعيل بروتوكول الـ **EIGRP** عليها , ولكن يجب أن نعلم لتتم هذه العملية بنجاح يجب أن تكون بعض الخطوات والمعلومات صحيح مثل يجب أن يكون الـ **AS** في الطرفين صحيح بمعني إذا كان **AS 1** يجب أن تكون **AS 1** في الطرف الآخر و الوثوقية في الطرفين صحيح و التوقيت ما بين الراوترات صحيح لتتم عملية البناء بشكل صحيح.

النموذج الكامل لعملية إرسال الحزم و بناء العلاقات ما بين الراوترات



المسار الرئيسي و المسار الاحتياطي

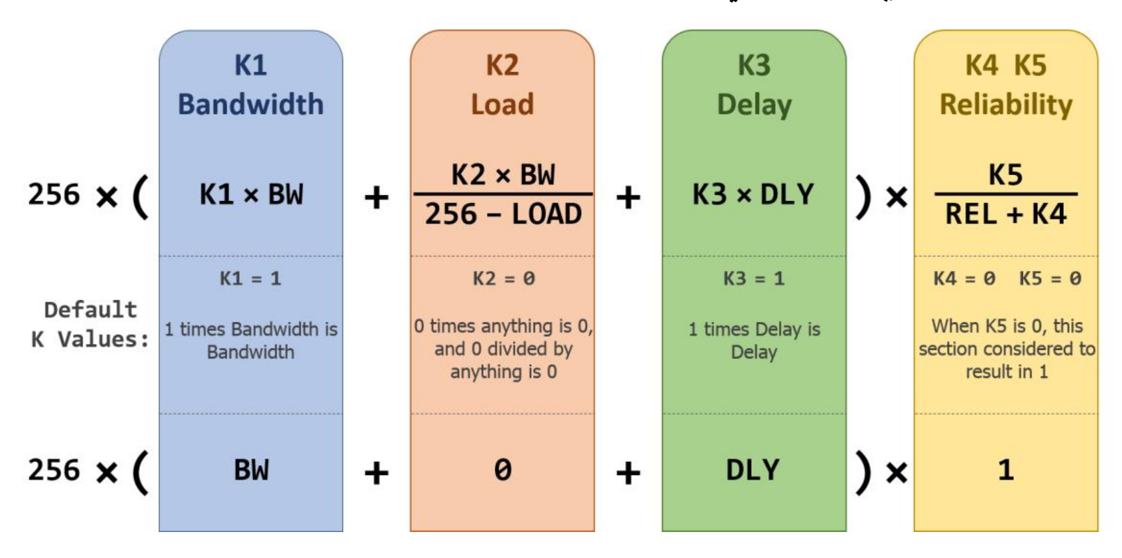
EIGRP Successor, Feasible Successor Routes



- تحديد المسار الرئيسي و المسار الاحتياطي في بروتوكول الـ **EIGRP** سنتعرف على كيفية الاختيار ما بين المسارات .

- **المسار الاساسي أو الرئيسي يسمى Successor.**
- **المسار الاحتياطي يسمى Feasible Successor.**

EIGRP Metric Calculation الحساب المتري الخاص في بروتوكول الـ



AS = Autonomous System

النظام المستقل ذاتياً

AS: هي عبارة عن مجموعة شبكات تخضع تحت نطاق واحد و تاخذ رقم خاص فيها و يكون تحت هذا النطاق مجموعة من الراوترات التي ترتبط في بعضها العبض و تشترك في رقم الـ **AS** واحد و في داخل هذه المنطقة يتم تفعيل بروتوكول الـ **EIGRP** على جميع الراوترات ليتم الاتصال في بعضهم البعض و في حال وجود فرع ثاني من الـ **AS** في منطقة اخرى و نريد أن نتصل في هذه المنطقة سنقوم بعمل إعدادات خاصة في موضوع الـ **Exterior** ليتم الربط ما بين المنطقة الداخلية و المنقطة الخارجية.

- أنواع الـ **AS** يوجد نوعان من الـ **AS** سأقوم بذكرهم و الشرح عنهم :

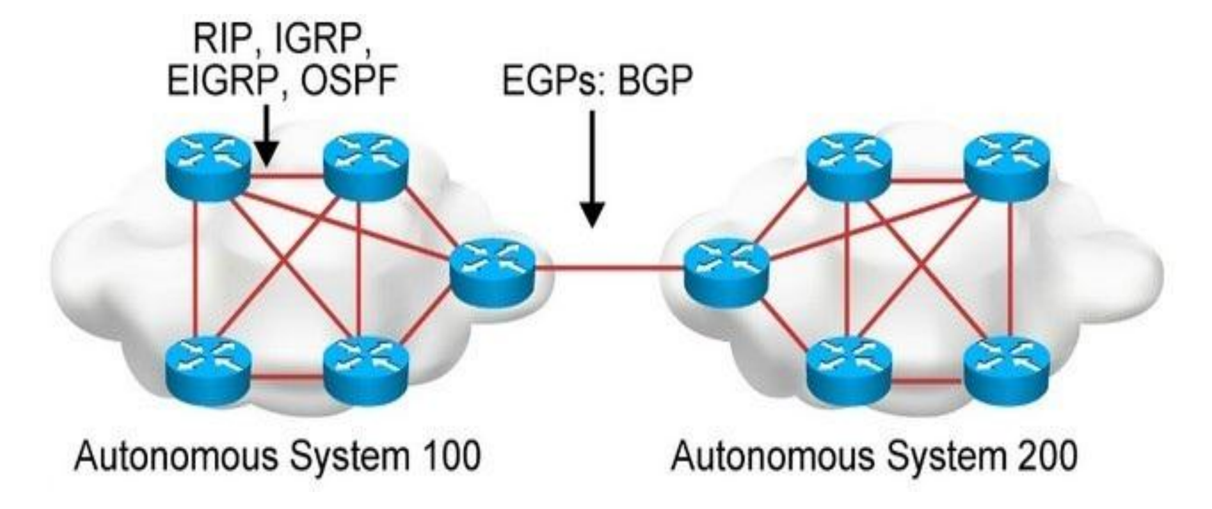
• النوع الأول **Interior Gateway Protocol** :

هذا النوع هو البوابة الداخلية بمعنى إنه يتم استخدام هذا النوع في الـ **AS** الداخلية و يعتمد على البروتوكولات الداخلية التي تربط الشبكات في بعضها البعض بشكل داخلي تحت نطاق واحد **AS** برقم معين و جميع الشبكات و الراوترات تحت هذا الـ **AS**.

• النوع الثاني **Exterior Gateway Protocol** :

هذا النوع هو البوابة الخارجية بمعنى إنه يربط المناطق في بعضهم البعض على مختلف الـ **AS** مثل لو كان لدنيا **AS 100** و **AS 200** و يتوجدون في مناطق مختلفة و بعيدة عن بعض و نريد أن نربط ما بينهم سنحتاج لبروتوكولات بوابة خارجية لنستطيع الربط ما بين هذه المناطق المختلفة و من اشهر هذه البروتوكولات المخصص للبوابة الخارجية **EGP** , **BGP** هذه البروتوكولات تستخدم للبوابة الخارجية .

- لاحظ في النموذج التالي إنه يوجد لدينا **AS 100** و **AS 200** في هذه الحالة يوجد لدينا شبكتان مختلفتان عن بعضهم البعض و كل شبكة تحت نطاق **AS** مختلف عن الآخر و لاحظ إنه في منتصف هذه الـ **AS** تم الربط ما بينهم من خلال بروتوكول بوابة خارجية مثل بروتوكول الـ **BGP** , **EGP** بهذا الشكل نكون قد فهمنا الـ **AS** .



EIGRP Key Technologies

التقنية التي يعتمد عليه بروتوكول الـ EIGRP

1- **Neighbor Discovery / Recovery (NDR)**
2- **Reliable Transport Protocol (RTP)**
3- **Diffusion Update Algorithm (Dual)**
4- **Protocol – Dependent Modules (PDM)**

- **Neighbor Discovery / Recovery:** هذه التقنية هي التي تسمح للراوترات أن تتعرف على بعضها البعض في داخل الشبكة و التي تعمل في نطاق واحد و المتصلة بشكل مباشر في الشبكة و يقوم الراوتر نفسه بتعريف عن نفسه ايضاً ليتم معرفة الراوترات التي تعمل في الشبكة و تبادل البيانات و المعلومات و المسارات في ما بين الراوترات و تعتمد هذه التقنية على رسالة الترحيب الـ **Hello Packets** إرسال و استقبال لتقوم بمعرفة التحديثات و التغيرات التي حصلت في الراوترات المجاورة.

- **Reliable Transport Protocol (RTP):** هذه التقنية المسؤولة عن حماية الـ **Packet** المرسلة ممن تجعل الـ **Packet** ترسل ثم تنتظر استلامه و تنظر الرد عليها هذه العملية تم تطبيقها في بروتوكول الـ **EIGRP** و هذه الرسالة لا يتم إرساله بشكل دوري.

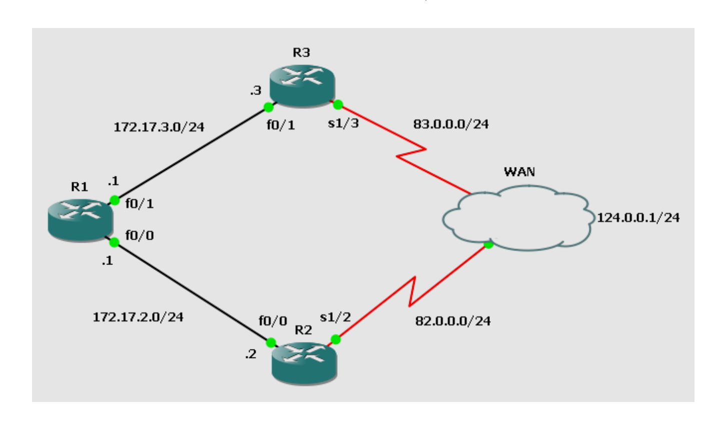
- **Diffusion Update Algorithm (Dual):** هذه التقنية تعتبر من أهم التقنية الموجودة في بروتوكول الـ **EIGRP** و هي تمثل العمود الفقري للبروتوكول لي لأنه تعتمد على الحركة الرئيسية حيث يتم في هذه التقنية اختيار افضل مسار ليكون المسار الرئيسي و يقوم ايضاً باختير المسار الاحتياطي أن وجد و يقوم ايضاً بعملية صيانة للمسارات و تحديد مسارات اخرى في حال حصل خطاء في أحد المسارات.

- **Protocol – Dependent Modules (PDM):** هذه التقنية التي تسمح لبروتوكول الـ **EIGRP** أن يتعمل مع الطبقة الثالثة **Network Layer 3** و تقوم ايضاً بعملية تغليف البيانات و ايضاً لتتم المحادثة مع البروتوكولات الآخر مثل **IPx** و **AppleTalk** .



EIGRP Load Balancing

توزيع الترافيك في بروتوكول الـ EIGRP

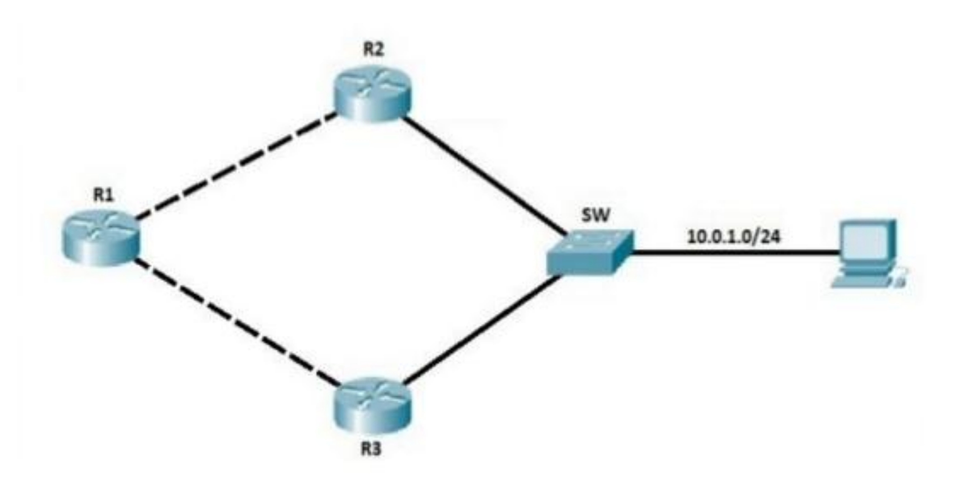


- **Load Balancing:** هي عملية توزيع الترافيك على عدة مسارات في الشبكة لتخفيف الحمل و ضغط على المسار الواحد الذي يرسل البيانات للشبكة المطلوبة.

- فائدة استخدام توزيع الترافيك في الشبكة هو تخفيف الضغط على المسارات مما يزيد من سرعة الشبكة في عملية الإرسال و الاستقبال هذه الفائدة الكبيرة من عملية توزيع الترافيك على عدة مسارات وايضاً تفيد في حال تعطل مسار سيتم اختيار مسار ثاني لخروج الترافيك منه و استلام الترافيك منه ايضاً .

- **مثال على توزيع الترافيك في عملية الـ Load Balancing :**
- يوجد لدينا هذا النموذج التالي سنقوم بشرح مثال عليه لنتعرف على كيفية توزيع الترافيك.

في هذا النموذج يوجد جهاز الحاسوب يريد الاتصال في شبكة اخرى على سبيل المثال و يريد أن يقوم بإرسال بيانات بشكل كبير سيقوم بإرسال البيانات على الشبكة و عندما تصل البيانات للراوتر سيقوم الراوتر بتوزيع البيانات على الراوتر **R2** و **R3** ليتم توزيع الترافيك و وصولها للشبكة الآخر التي يربطها الراوتر **R1** بهذا الشكل يكون قد تم توزيع الترافيك و تخفيف الضغط على المسار الواحد .



تقنية الـ Passive Interface

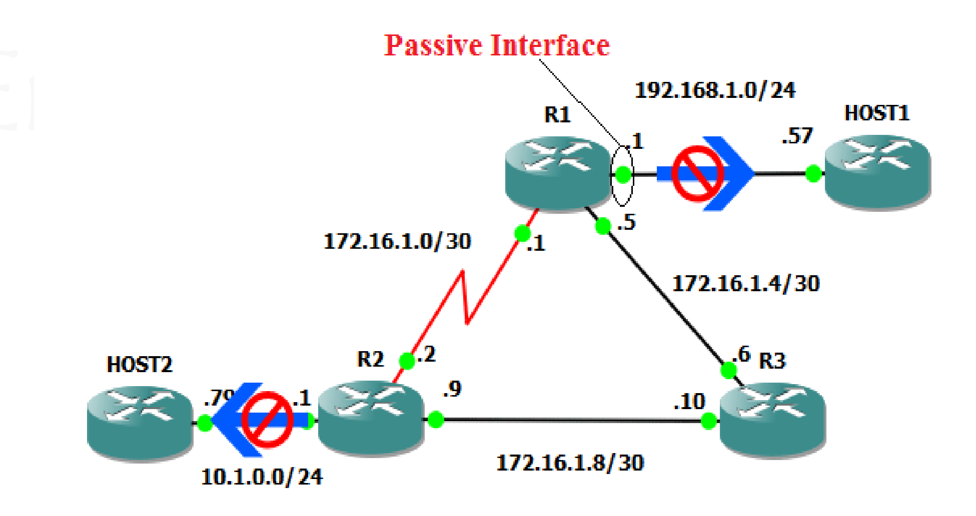
عملية قفل المنفذ

- **فكرة الـ Passive Interface :** هي فكرة عامة موجودة في بروتوكولات التوجيه بشكل عام و، تستخدم لقفل منافذ معينة موجود في الراوترات لمنع هذا المنافذ أن تقوم بإرسال البيانات منه أو إرسال معلومات .

- تفيد هذه الفكرة في منع البيانات من الخروج مثل لو كان لدنيا راوتر متصل في هذا المنفذ ولا نريد أن يصله بيانات ، أو معلومات فقط نقوم بعمل فكرة الـ **Passive Interface** على المنفذ مما يجعل المنفذ مقفل غير قادر على الإرسال أو الاستقبال.

أنظر للنموذج التالي يوجد عدة شبكات و نريد قفل المنفذ المتصل في راوتر **R1** المتصل في راوتر الـ **HOST1** ليتم قفل المنفذ و منع خروج البيانات منه سنقوم بكتابة الأمر التالي في داخل الراوتر **R1** ...

Router (config) # **router eigrp 1**
Router (config -router) # **passive-interface fastethernet 0/1**



- بهذه الطريقة يكون قد تم قفل المنفذ **f 0/1** الموجود على راوتر **R1** لمنع خروج البيانات من المنفذ للراوتر الـ **HOST1**.

- **ملاحظة مهم جداً جداً :** عند تفعيل هذه الخاصية على بروتوكول الـ **EIGRP** في هذه الحالة يجب أن نعرف إنه سيتم قطع العلاقة ما بين الراوتر الذي تم تنفيذ هذا الأمر عليه و الراوتر الآخر المتصل فيه و يجب أن نكون على معرفة قبل أن نقع في مشاكل.

- إعدادات بروتوكول EIGRP Configuration :

Router > **enable**

Router # **config t**

Router (config) # **router eigrp 1** → **AS number 1**

Router (config-router) # **network 192.168.1.0**

Router (config-router) # **network 192.168.2.0**

Router (config-router) # **exit**

Router # **show ip route**

هذا الأمر لعرض جدول التوجيه

Router # **show ip eigrp topology**

هذا الأمر لعرض الراوترات المجاورة الموجودة في الشبكة

Router # **show ip eigrp neighbors**

هذا الأمر لعرض قاعدة البيانات أو الطوبولوجي التي مسجل فيه كل معلومات الشبكة

EIGRP Configuration, Network BMA

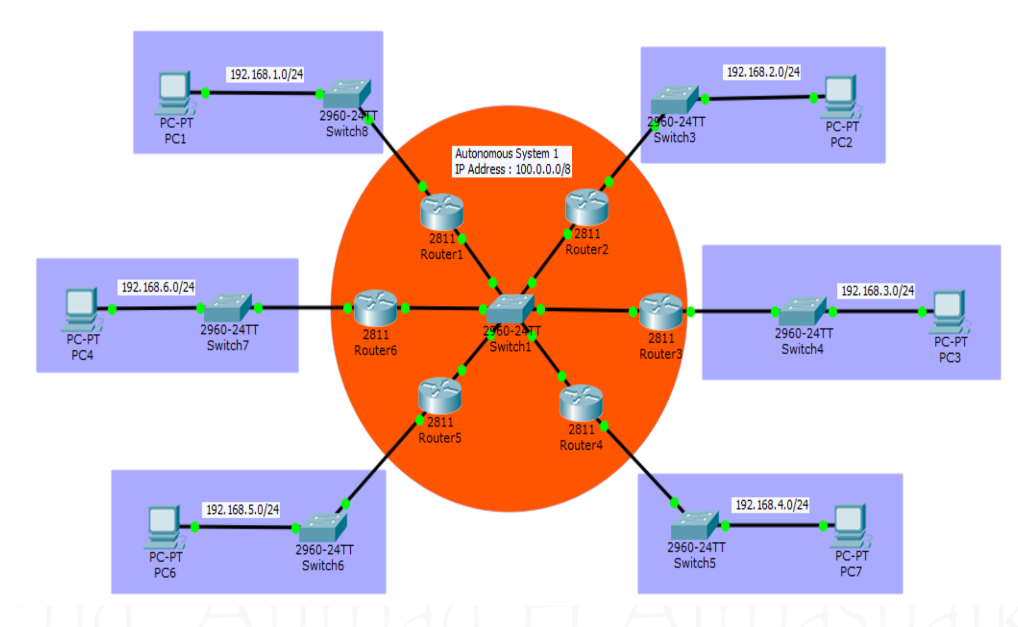
إعدادات بروتوكول الـ EIGRP على الشبكة السريعة

- **الأن سنقوم بتفعيل الـ EIGRP على شبكة مكونة من 7 شبكات و سيتواجد نموذج للعمل عليه .**
- **في البداية يجب معرفة الإعدادات التي سيتم العمل عليها و معرفة الشبكات الـ 7 و معرفة الـ AS لنقوم بتفعيل البروتوكول على الشبكة بشكل صحيح:**

١. الشبكة الأولى ستكون بعنوان **192.168.1.0/24** .
٢. الشبكة الثانية ستكون بعنوان **192.168.2.0/24** .
٣. الشبكة الثالثة ستكون بعنوان **192.168.3.0/24** .
٤. الشبكة الرابعة ستكون بعنوان **192.168.4.0/24** .
٥. الشبكة الخامسة ستكون بعنوان **192.168.5.0/24** .
٦. الشبكة السادسة ستكون بعنوان **192.168.6.0/24** .
٧. الشبكة السابعة ستكون بعنوان **100.0.0.0/8** هذه الشبكة التي سترتبط الراوترات مع بعضها البعض و تكون في داخل شبكة واحدة و نطاق واحد .
٨. ستكون جميع الشبكات في داخل نطاق واحد بمعنى **AS 1** .

الأن بعد أن تعرفنا على الشبكات و الإعدادات سنقوم بعمل إعدادات و تشغيل الإنترفيس و تركيب الاي بي على جميع الإنترفيس الموجودة على الراوترات ، و بعدها سنقوم بتفعيل بروتوكول الـ **EIGRP** لتسطيع جميع الشبكات الاتصال مع بعضها البعض مثل ما في النموذج التالي المرفق اسفل ، وسنقوم بتعريف الشبكات في الراوترات ليتم إضافة عناوين الشبكات في جداول التوجيه ليتم الاتصال و التعرف على الشبكات بشكل صحيح .

النموذج التالي هو الذي سيتم العمل عليه



- الأن سنقوم بدخول على **R1** و عمل الإعدادات التالية :

الأن سنقوم بكتابة الاوامر التالية :

Router > **enable**

Router # **config t**

Router (config) # **interface fastethernet 0/0**

Router (config-if) # **ip address 100.0.0.1 255.0.0.0**

Router (config-if) # **no shutdown**

Router (config-if) # **exit**

Router (config) # **interface fastethernet 0/1**

Router (config-if) # **ip address 192.168.1.1 255.255.255.0**

Router (config-if) # **no shutdown**

Router (config-if) # **exit**

Router (config) # **router eigrp 1**

Router (config-router) # **network 100.0.0.0**

Router (config-router) # **network 192.168.1.0**

Router (config- router) # **end**

Router # **copy running-config startup-config**

هذه إعدادات الراوتر الأول **R1** كاملة الأن سنقوم بدخول للراوتر الثاني **R2** لنقوم بعمل الإعدادات .

- الأن سنقوم بدخول على **R2** و عمل الإعدادات التالية :

الأن سنقوم بكتابة الاوامر التالية :

Router > **enable**

Router # **config t**

Router (config) # **interface fastethernet 0/0**

Router (config-if) # **ip address 100.0.0.2 255.0.0.0**

Router (config-if) # **no shutdown**

Router (config-if) # **exit**

Router (config) # **interface fastethernet 0/1**

Router (config-if) # **ip address 192.168.2.1 255.255.255.0**

Router (config-if) # **no shutdown**

Router (config-if) # **exit**

Router (config) # **router eigrp 1**

Router (config-router) # **network 100.0.0.0**

Router (config-router) # **network 192.168.2.0**

Router (config- router) # **end**

Router # **copy running-config startup-config**

هذه إعدادات الراوتر الأول **R2** كاملة الأن سنقوم بدخول للراوتر الثاني **R3** لنقوم بعمل الإعدادات .

- الأن سنقوم بدخول على **R3** و عمل الإعدادات التالية :

الأن سنقوم بكتاية الاوامر التالية :

Router > **enable**

Router # **config t**

Router (config) # **interface fastethernet 0/0**

Router (config-if) # **ip address 100.0.0.3 255.0.0.0**

Router (config-if) # **no shutdown**

Router (config-if) # **exit**

Router (config) # **interface fastethernet 0/1**

Router (config-if) # **ip address 192.168.3.1 255.255.255.0**

Router (config-if) # **no shutdown**

Router (config-if) # **exit**

Router (config) # **router eigrp 1**

Router (config-router) # **network 100.0.0.0**

Router (config-router) # **network 192.168.3.0**

Router (config- router) # **end**

Router # **copy running-config startup-config**

هذه إعدادات الراوتر الثالث **R3** كاملة الأن سنقوم بدخول للراوتر الثاني **R4** لنقوم بعمل الإعدادات .

- الأن سنقوم بدخول على **R4** و عمل الإعدادات التالية :

الأن سنقوم بكتاية الاوامر التالية :

Router > **enable**

Router # **config t**

Router (config) # **interface fastethernet 0/0**

Router (config-if) # **ip address 100.0.0.4 255.0.0.0**

Router (config-if) # **no shutdown**

Router (config-if) # **exit**

Router (config) # **interface fastethernet 0/1**

Router (config-if) # **ip address 192.168.4.1 255.255.255.0**

Router (config-if) # **no shutdown**

Router (config-if) # **exit**

Router (config) # **router eigrp 1**

Router (config-router) # **network 100.0.0.0**

Router (config-router) # **network 192.168.4.0**

Router (config- router) # **end**

Router # **copy running-config startup-config**

هذه إعدادات الراوتر الرابع **R4** كاملة الأن سنقوم بدخول للراوتر الخامس **R5** لنقوم بعمل الإعدادات .

- الأن سنقوم بدخول على **R5** و عمل الإعدادات التالية :

الأن سنقوم بكتابة الاوامر التالية :

Router > **enable**

Router # **config t**

Router (config) # **interface fastethernet 0/0**

Router (config-if) # **ip address 100.0.0.5 255.0.0.0**

Router (config-if) # **no shutdown**

Router (config-if) # **exit**

Router (config) # **interface fastethernet 0/1**

Router (config-if) # **ip address 192.168.5.1 255.255.255.0**

Router (config-if) # **no shutdown**

Router (config-if) # **exit**

Router (config) # **router eigrp 1**

Router (config-router) # **network 100.0.0.0**

Router (config-router) # **network 192.168.5.0**

Router (config- router) # **end**

Router # **copy running-config startup-config**

هذه إعدادات الراوتر الخامس **R5** كاملة الأن سنقوم بدخول للراوتر السادس **R6** لنقوم بعمل الإعدادات .

- الأن سنقوم بدخول على **R6** و عمل الإعدادات التالية :

الأن سنقوم بكتابة الاوامر التالية :

Router > **enable**

Router # **config t**

Router (config) # **interface fastethernet 0/0**

Router (config-if) # **ip address 100.0.0.6 255.0.0.0**

Router (config-if) # **no shutdown**

Router (config-if) # **exit**

Router (config) # **interface fastethernet 0/1**

Router (config-if) # **ip address 192.168.6.1 255.255.255.0**

Router (config-if) # **no shutdown**

Router (config-if) # **exit**

Router (config) # **router eigrp 1**

Router (config-router) # **network 100.0.0.0**

Router (config-router) # **network 192.168.6.0**

Router (config- router) # **end**

Router # **copy running-config startup-config**

هذه إعدادات الراوتر السادس **R6** كاملة و الاخير وبهذا الشكل نكون قد تم الانتهاء من برمجة جميع الراوترات و تفعيل بروتوكول الـ **EIGRP** على جميع الراوترات.

- الأن بعد الانتهاء من برمجة جميع الراوترات يجب أن نتاكد هل تم إضافة جميع الشبكات في جميع الراوترات أو لا و نريد أن نقوم بعمل اختبار ما بين الشبكات كلها لنتاكد هل الشبكات تستطيع الاتصال مع بعضها البعض، أو لا سنقوم بدخول على الراوتر الأول و نقوم بدخول على جدول التوجيه و نتاكد هل تم إضافة جميع الشبكات أو لا .

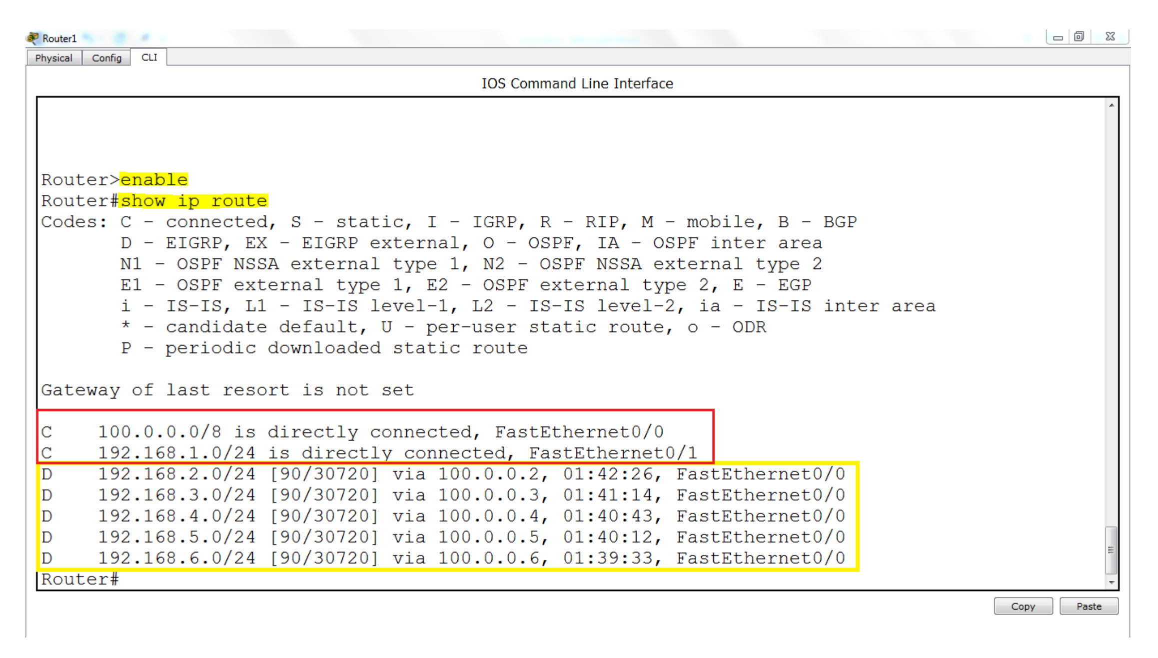
- **ملاحظة مهم جداً جداً :** رمز بروتوكول الـ **EIGRP** في جدول التوجيه **D** عندما نرى رمز **D** في جدول التوجيه يجب أن نعرف إنه تم تفعيل بروتوكول الـ **EIGRP**.

- الأن سنقوم بدخول على **R1** و نقوم بكتابة الأمر التالي لعرض جدول التوجيه :

Router > **enable**

Router # **show ip route**

R1



```
Router>enable
Router#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

C    100.0.0.0/8 is directly connected, FastEthernet0/0
C    192.168.1.0/24 is directly connected, FastEthernet0/1
D    192.168.2.0/24 [90/30720] via 100.0.0.2, 01:42:26, FastEthernet0/0
D    192.168.3.0/24 [90/30720] via 100.0.0.3, 01:41:14, FastEthernet0/0
D    192.168.4.0/24 [90/30720] via 100.0.0.4, 01:40:43, FastEthernet0/0
D    192.168.5.0/24 [90/30720] via 100.0.0.5, 01:40:12, FastEthernet0/0
D    192.168.6.0/24 [90/30720] via 100.0.0.6, 01:39:33, FastEthernet0/0
Router#
```

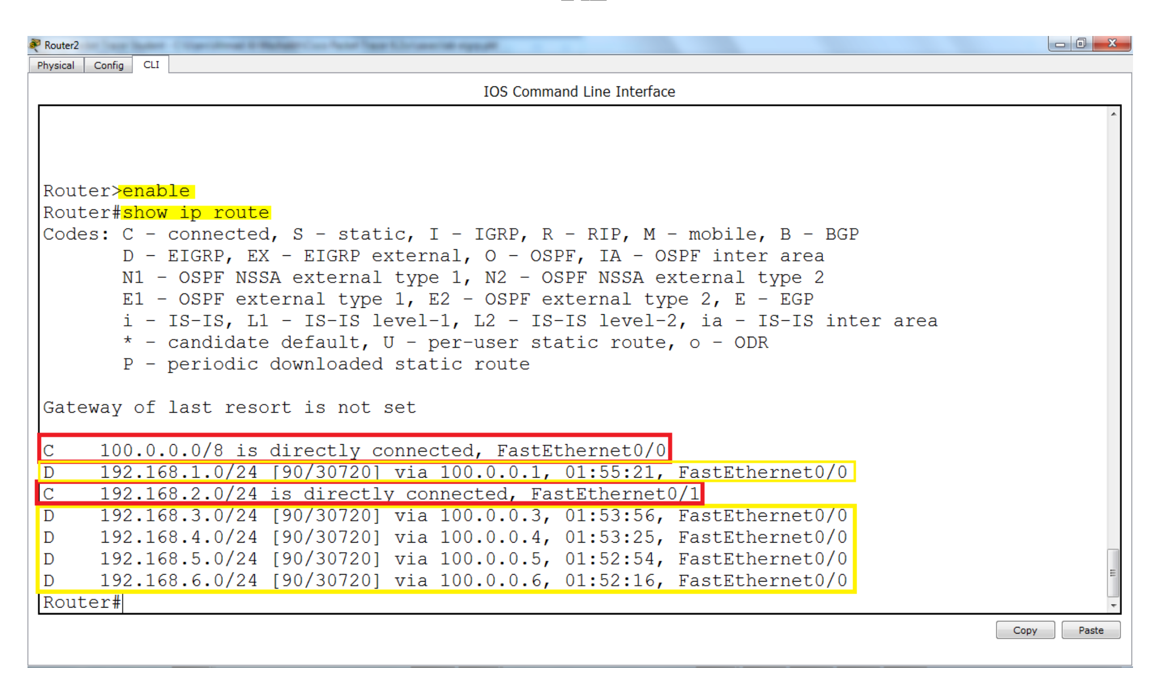
- لاحظ الأن بعد الدخول على **R1** و كتابة امر عرض جدول التوجيه لاحظ إنه يوجد **7** شبكات متصلة في الراوتر الأول **R1** و يستطيع ايضاً هذا الراوتر الاتصال في الشبكات الموجودة في الجدول المحددة بالون الاصفر هذه الشبكات التي تم اضافتها من خلال بروتوكول الـ **EIGRP** و يجب أن نعرف أن هذه الشبكات من الطبيعي جداً إنه على الراوترات الباقية أو المجاورة تم تفعيل بروتوكول الـ **EIGRP** على جميع الراوترات الموجودة في الشبكة و إذا قمنا بدخول على جميع الراوترات سنجد أن جميع الراوترات تحتوي على الـ **7** شبكات , و بنسبه للشبكات المحددة بالون الاحمر هذه الشبكات المتصلة في الراوتر اتصال مباشر من دون بروتوكول الـ **EIGRP** .

- الأن سنقوم بدخول على **R2** و نقوم بكتابة الأمر التالي لعرض جدول التوجيه :

Router > **enable**

Router # **show ip route**

R2



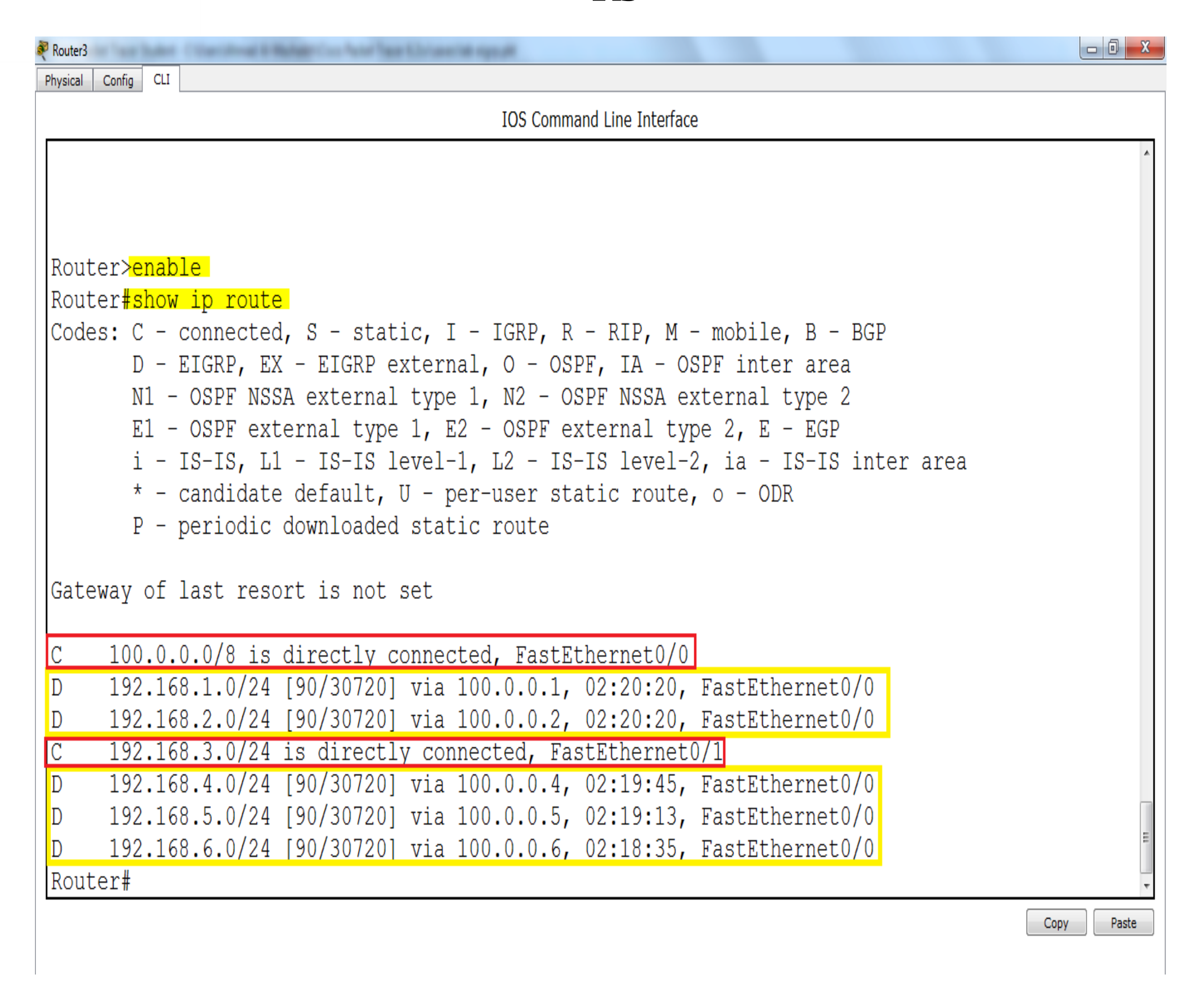
- لاحظ الآن قمنا بدخول على **R2** و قمنا بكتابة امر عرض جدول التوجيه تم عرض **7** شبكات ايضاً هذا يدل على أن الراوتر الثاني **R2** قام ايضاً بتحديث جدول التوجيه لديه و قام بإضافة الشبكات .
- اريد أن اوضح نقطة مهم جداً أنظر للشبكات كل شبكة يتساوى على الجانب الآخر لديها عنوان شبكة **100.0.0.0/8** هذا عنوان الشبكة الداخلية التي تربط جميع الراوترات في شبكة واحدة على سويتش واحد ، و نطاق واحد و في هذه الحالة يجب أن نعرف إنه اي شبكة من هذه الشبكة لو ارادت أن تتصل في أحد الشبكات ستقوم بتوصيل عن طريق شبكة **100.0.0.0/8** المسؤولة عن الربط ما بين الشبكات ، و لاحظ إنه كل شبكة تاخذ عنوان متشابه من نفس النطاق و نفس رنج الاي بي مثل **100.0.0.1** و **100.0.0.2** و ما بعدهم من هذه العناوين هذا لي لأنهم في نطاق واحد و في شبكة بث مباشرة واحدة تسمى هذه الشبكة **BMA** و في هذه الحالة يجب أن تكون جميع العناوين في نطاق واحد ليتم العمل بشكل صحيح .

- الأن سنكمل عملية استكشاف جداول التوجيه في الراوترات التالية **R3** و **R4** و **R5** و **R6** لنرى و نتاكد هل تم إضافة جميع الشبكات أو لا سنقوم بدخول عليهم واحد واحد و نقوم بكتابة امر عرض جدول التوجيه التالي :

Router > **enable**

Router # **show ip route**

R3

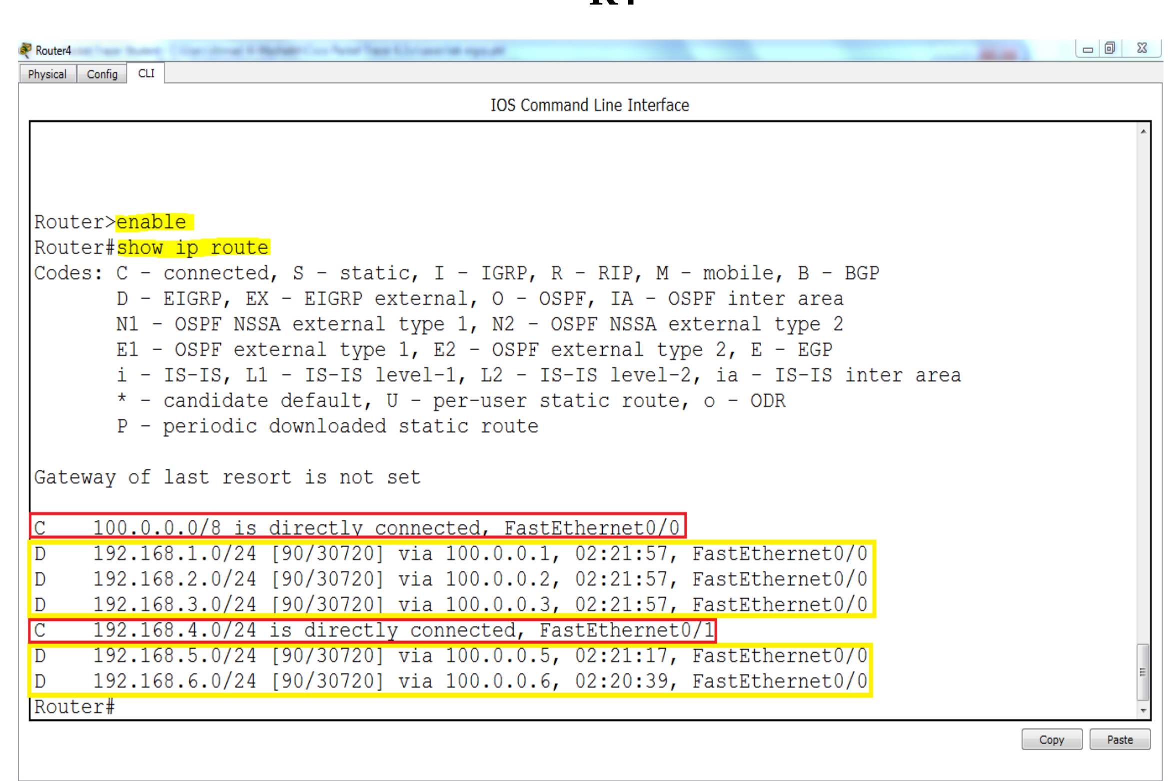


```
Router>enable
Router#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

C    100.0.0.0/8 is directly connected, FastEthernet0/0
D    192.168.1.0/24 [90/30720] via 100.0.0.1, 02:20:20, FastEthernet0/0
D    192.168.2.0/24 [90/30720] via 100.0.0.2, 02:20:20, FastEthernet0/0
C    192.168.3.0/24 is directly connected, FastEthernet0/1
D    192.168.4.0/24 [90/30720] via 100.0.0.4, 02:19:45, FastEthernet0/0
D    192.168.5.0/24 [90/30720] via 100.0.0.5, 02:19:13, FastEthernet0/0
D    192.168.6.0/24 [90/30720] via 100.0.0.6, 02:18:35, FastEthernet0/0
Router#
```

R4

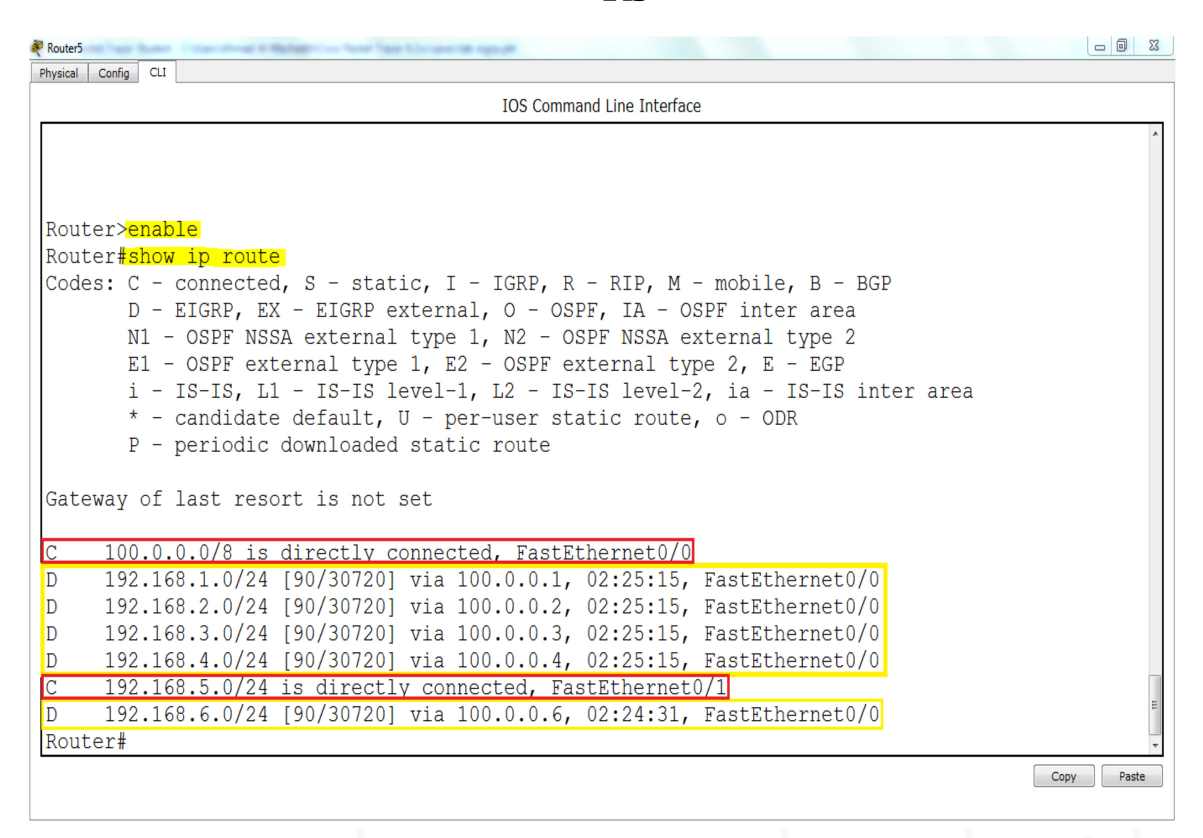


```
Router>enable
Router#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

C    100.0.0.0/8 is directly connected, FastEthernet0/0
D    192.168.1.0/24 [90/30720] via 100.0.0.1, 02:21:57, FastEthernet0/0
D    192.168.2.0/24 [90/30720] via 100.0.0.2, 02:21:57, FastEthernet0/0
D    192.168.3.0/24 [90/30720] via 100.0.0.3, 02:21:57, FastEthernet0/0
C    192.168.4.0/24 is directly connected, FastEthernet0/1
D    192.168.5.0/24 [90/30720] via 100.0.0.5, 02:21:17, FastEthernet0/0
D    192.168.6.0/24 [90/30720] via 100.0.0.6, 02:20:39, FastEthernet0/0
Router#
```

R5



```
Router5
Physical  Config  CLI
IOS Command Line Interface

Router>enable
Router#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

C    100.0.0.0/8 is directly connected, FastEthernet0/0
D    192.168.1.0/24 [90/30720] via 100.0.0.1, 02:25:15, FastEthernet0/0
D    192.168.2.0/24 [90/30720] via 100.0.0.2, 02:25:15, FastEthernet0/0
D    192.168.3.0/24 [90/30720] via 100.0.0.3, 02:25:15, FastEthernet0/0
D    192.168.4.0/24 [90/30720] via 100.0.0.4, 02:25:15, FastEthernet0/0
C    192.168.5.0/24 is directly connected, FastEthernet0/1
D    192.168.6.0/24 [90/30720] via 100.0.0.6, 02:24:31, FastEthernet0/0
Router#
Copy  Paste
```


R6

```
Router6
Physical  Config  CLI
IOS Command Line Interface

Router>enable
Router#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

C    100.0.0.0/8 is directly connected, FastEthernet0/0
D    192.168.1.0/24 [90/30720] via 100.0.0.1, 02:27:22, FastEthernet0/0
D    192.168.2.0/24 [90/30720] via 100.0.0.2, 02:27:22, FastEthernet0/0
D    192.168.3.0/24 [90/30720] via 100.0.0.3, 02:27:22, FastEthernet0/0
D    192.168.4.0/24 [90/30720] via 100.0.0.4, 02:27:22, FastEthernet0/0
D    192.168.5.0/24 [90/30720] via 100.0.0.5, 02:27:22, FastEthernet0/0
C    192.168.6.0/24 is directly connected, FastEthernet0/1
Router#
Copy  Paste
```

- الأن بعد أن قمنا بعرض جداول التوجيه لجميع الراوترات نرى إنه يوجد في كل الراوترات 7 شبكات وجميعهم متصلين في بعضهم البعض عن طريق شبكة الـ 100.0.0.0/8 طبعاً و الاعتماد على بروتوكول الـ EIGRP في عملية تعريف و توصيل الشبكات في بعضها البعض.

- بعد أن قمنا بتطبيق العملي على عنوان الـ IPv4 للبروتوكولات السابقة ، الأن سنقوم بتطبيق العملي على عنوان الـ IPv6 للبروتوكولات التالية :

١- IP Address v6
٢- Static Router IPv6
٣- Routing Information Protocol Next Generation (RIPng)
٤- Enhanced Interior Gateway (EIGRP)
٥- Open Shortest Path First (OSPFv3)

سنتعرف على إعدادات البروتوكولات و الإعدادات اليدوية كما هو موجود في الاعلى :

Static Router IPv6


```
Router > enable

Router # config t

Router (config) # ipv6 unicast-routing

Router (config) # interface fastethernet 0/0

Router (config-if) # ipv6 address fec0::1/64

Router (config) # ipv6 route fec0:1::/64 2005::2

Router (config) # show ipv6 route
```

- الأن بعد أن تعرفنا على إعدادات التوجيه اليدوي سنقوم بتطبيق الإعدادات على نموذج مكون من راوترين ، و ثلاث شبكات تعمل بعنوان الإصدار السادس IPv6 و سنقوم بتعرف على إعدادات الشبكة لنبدأ بعدها بعملية التطبيق .

- **الإعدادات التي سيتم بناء الشبكة عليها .**

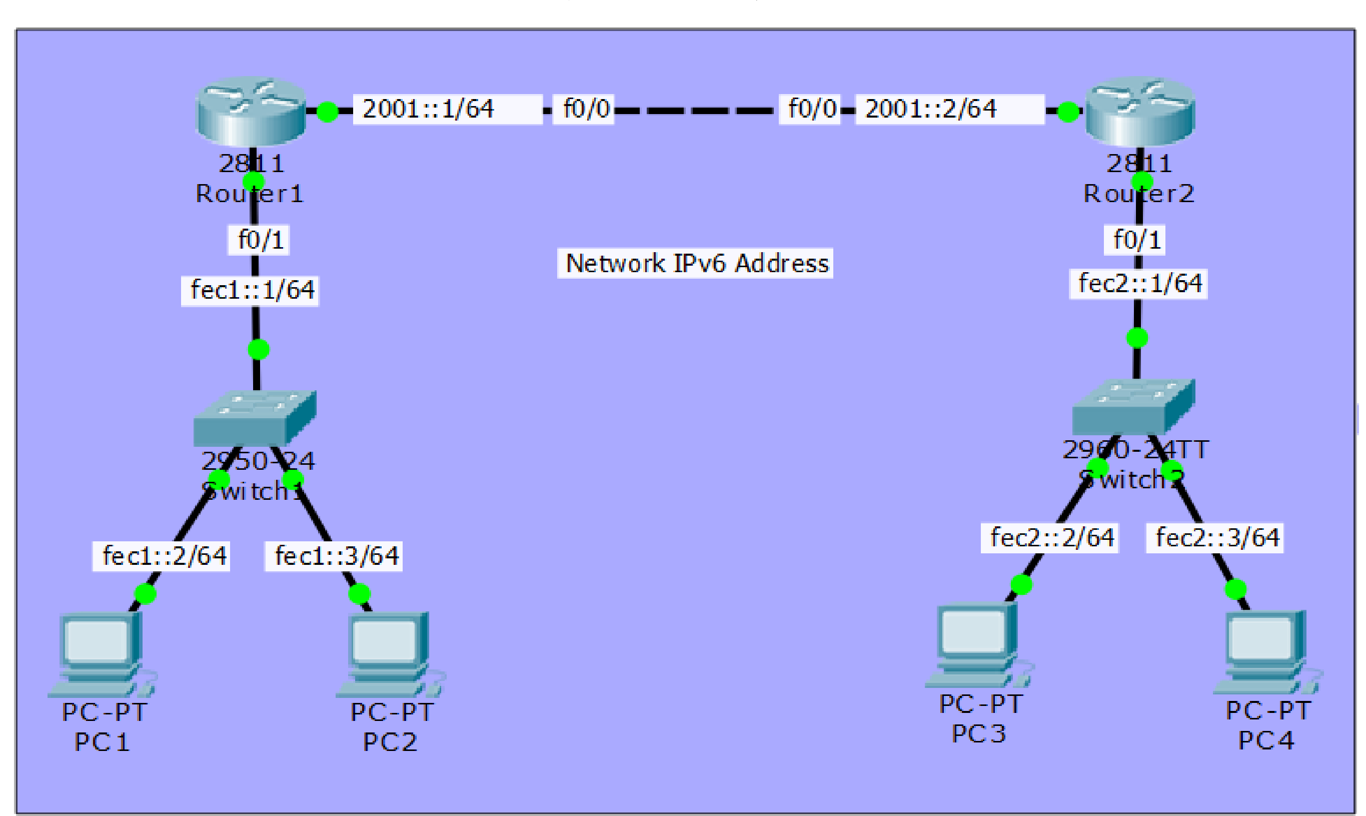
- **في البداية يجب معرفة الإعدادات التي سيتم العمل عليها و معرفة الشبكات الـ 3 :**

١- الشبكة الأولى ستكون بعنوان **fec1::1/64**
٢- الشبكة الثانية ستكون بعنوان **fec2::1/64**
٣- الشبكة الثالثة ستكون بعنوان **2001::1 /64**

هذه إعدادات الشبكة كلها ويجب أن نعلم أن الشبكة الثالثة هي التي سترتبط ما بين الشبكة الأولى و الثاني ، ليتم الاتصال فيما بينهم بعد أن نقوم بعملية التوجيه .

الأن بعد أن تعرفنا على الشبكات و الإعدادات سنقوم بعمل إعدادات و تشغيل الإنترفيس و تركيب الاي بي على جميع الإنترفيس الموجودة على الراوترات و بعده سنقوم بعمل إعدادات التوجيه اليدوي لبناء جدول التوجيه ، لتسطيع جميع الشبكات الاتصال مع بعضها البعض مثل ما في النموذج التالي المرفق اسفل وسنقوم بإضافة الشبكات في الراوترات ليتم إضافة عناوين الشبكات في جداول التوجيه ليتم الاتصال و التعرف على الشبكات بشكل صحيح .

النموذج التالي هو الذي سيتم العمل عليه



- **الأن سنقوم بدخول على الراوتر الأول R1 و نقوم بكتابة الإعدادات التالية :**

سنقوم بكتابة الاومر التالية :

Router> **enable**

Router # **config t**

Router (config) # **ipv6 unicast-routing**

Router (config) # **interface fastethernet 0/0**

Router (config-if) # **ipv6 address 2001::1/64**

Router (config-if) # **no shutdown**

Router (config-if) # **exit**

Router (config) # **interface fastethernet 0/1**

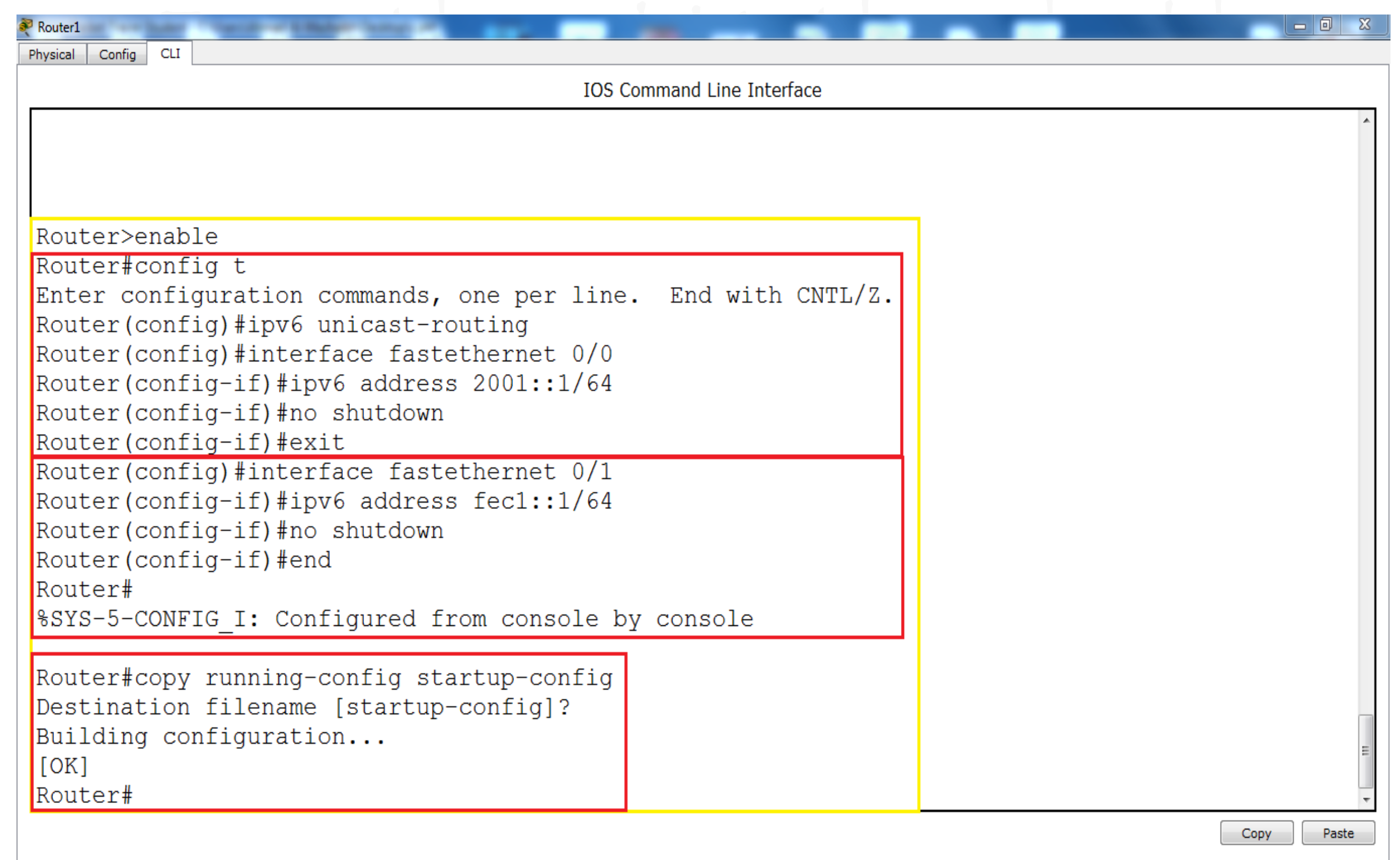
Router (config-if) # **ipv6 address fce1::1/64**

Router (config-if) # **no shutdown**

Router (config-if) # **end**

Router # **copy running-config startup-config**

- هذه إعدادات الراوتر الأول ، مع العلم لم نقم بعد بعملية إعدادات التوجيه اليدوي، كما في الصورة التالية من داخل **R1**:



- **الأن سنقوم بدخول على الراوتر الثاني R2 و نقوم بكتابة الإعدادات التالية :**

سنقوم بكتابة الاومر التالية :

Router> **enable**

Router # **config t**

Router (config) # **ipv6 unicast-routing**

Router (config) # **interface fastethernet 0/0**

Router (config-if) # **ipv6 address 2001::2/64**

Router (config-if) # **no shutdown**

Router (config-if) # **exit**

Router (config) # **interface fastethernet 0/1**

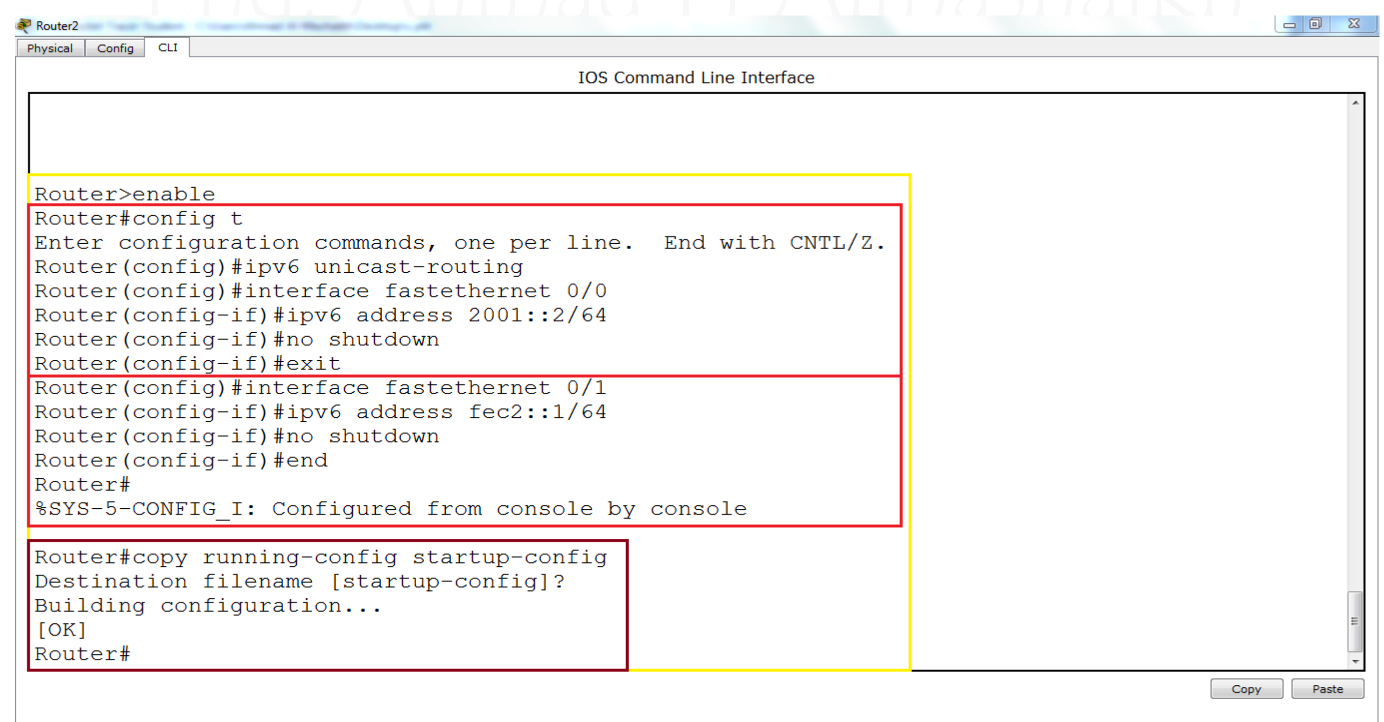
Router (config-if) # **ipv6 address fce2::1/64**

Router (config-if) # **no shutdown**

Router (config-if) # **end**

Router # **copy running-config startup-config**

هذه إعدادات الراوتر الثاني ، مع العلم لم نقم بعد بعملية إعدادات التوجيه اليدوي ، كما في الصورة التالية من داخل **R2** :



```
Router>enable
Router#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#ipv6 unicast-routing
Router(config)#interface fastethernet 0/0
Router(config-if)#ipv6 address 2001::2/64
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#interface fastethernet 0/1
Router(config-if)#ipv6 address fec2::1/64
Router(config-if)#no shutdown
Router(config-if)#end
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
Router#
```

- بهذا الشكل من الإعدادات نكون قد قمنا ببرمجة الراوترات ، و قمنا بتشغيل الإنترفيس و تركيب العناوين الخاصة في الإصدار السادس و يتبقى علينا الأن أن نقوم بعملية إعدادات التوجيه اليدوي لتستطيع الشبكات أن تتصل مع بعضها البعض من خلال الشبكة الثلاثة.

- الأن سنقوم بدخول على الراوتر الأول **R1** و نقوم بكتابة الإعدادات التالية :

سنقوم بكتابة الاومر التالية :

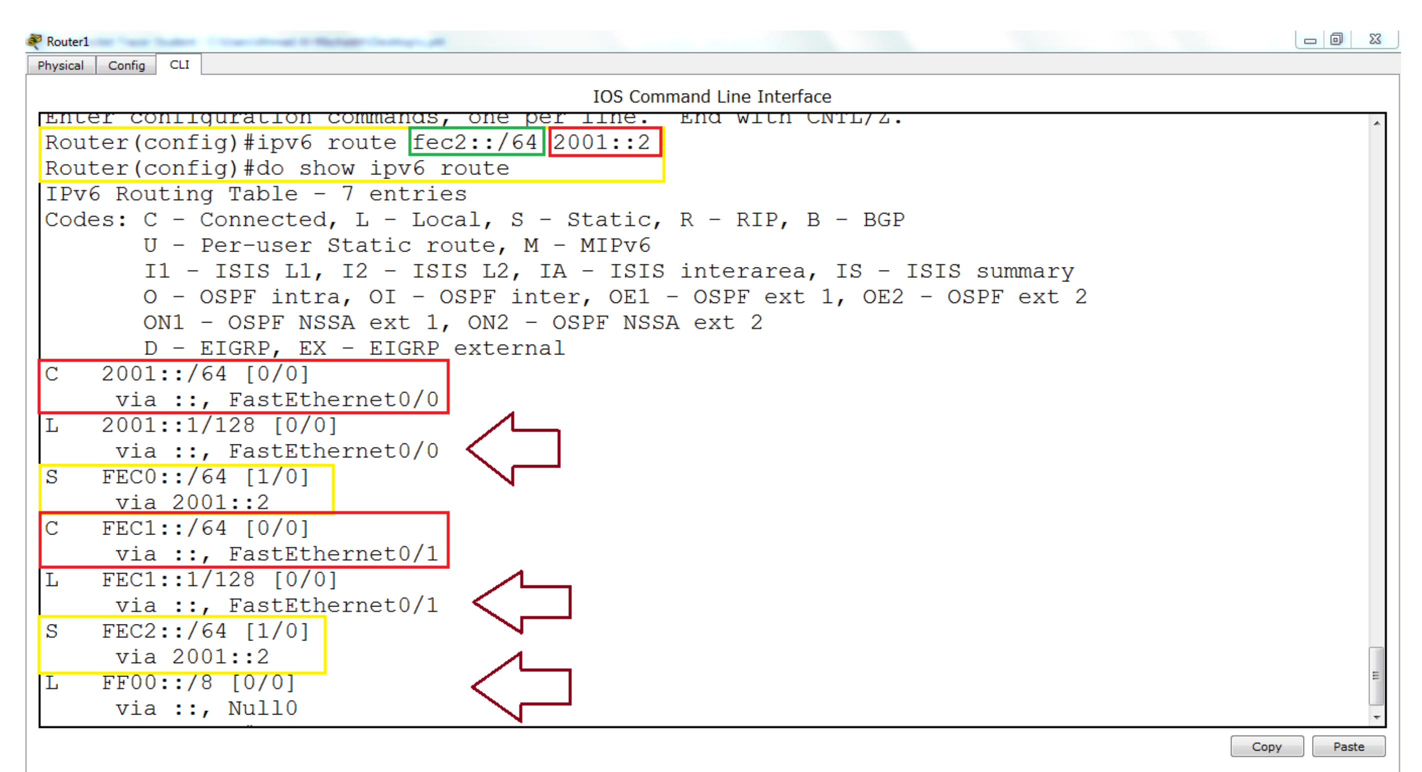
Router > **enable**

Router # **config t**

Router (config) **# ipv6 route fec2::/64 2001::2** **هذه امر التوجيه اليدوي**

Router (config) # **do show ipv6 route** **لعرض جدول التوجيه**

هذه إعدادات التوجيه اليدوي في الرواتر الأول **R1** كما في الصورة التالية من داخل الراوتر الأول **R1** :



- لاحظ بعد عرض جدول التوجيه يوجد لدنيا أكثر من شبكة و كل شبكة تاخذ رمز مختلف عن الآخر ، مثل الشبكة التي تاخذ رمز **C** يجب أن نعرف إنه الشبكة المتصلة بجهز الراوتر بشكل مباشر و من دون إعدادات التوجيه لا عن طريق بروتوكول ولا عن طريق التوجيه اليدوي ، بينما الشبكة التي تاخذ رمز **S** هي الشبكة التي تم اضافتها عن طريق التوجيه اليدوي و رمز **S** هو اختصار لـ **Static** ، و الشبكة التي تاخذ رمز **L** هي الشبكة الداخلية التي تمثل شبكة الـ **APIPA** في عنوان الإصدار الرابع بينما في الإصدار السادس تم تغير الاسم و قمنا بشرح هذه المعلومات في الدروس السابقة ، الأن لو جهاز حاسوب موجود في شبكة بعنوان **FEC1::2/64** يريد الاتصال بجهاز موجود في شبكة بعنوان **FEC2::2/64** سيتم ما بين هذه الشبكة عن طريق الشبكة الثالثة و هي الشبكة التي تربط ما بينهم و تاخذ عنوان **2001::1/64**.

- الأن سنقوم بدخول على الراوتر الثاني **R2** و نقوم بكتابة الإعدادات التالية لعملية أعداد التوجيه اليدوي :

سنقوم بكتابة الاومر التالية :

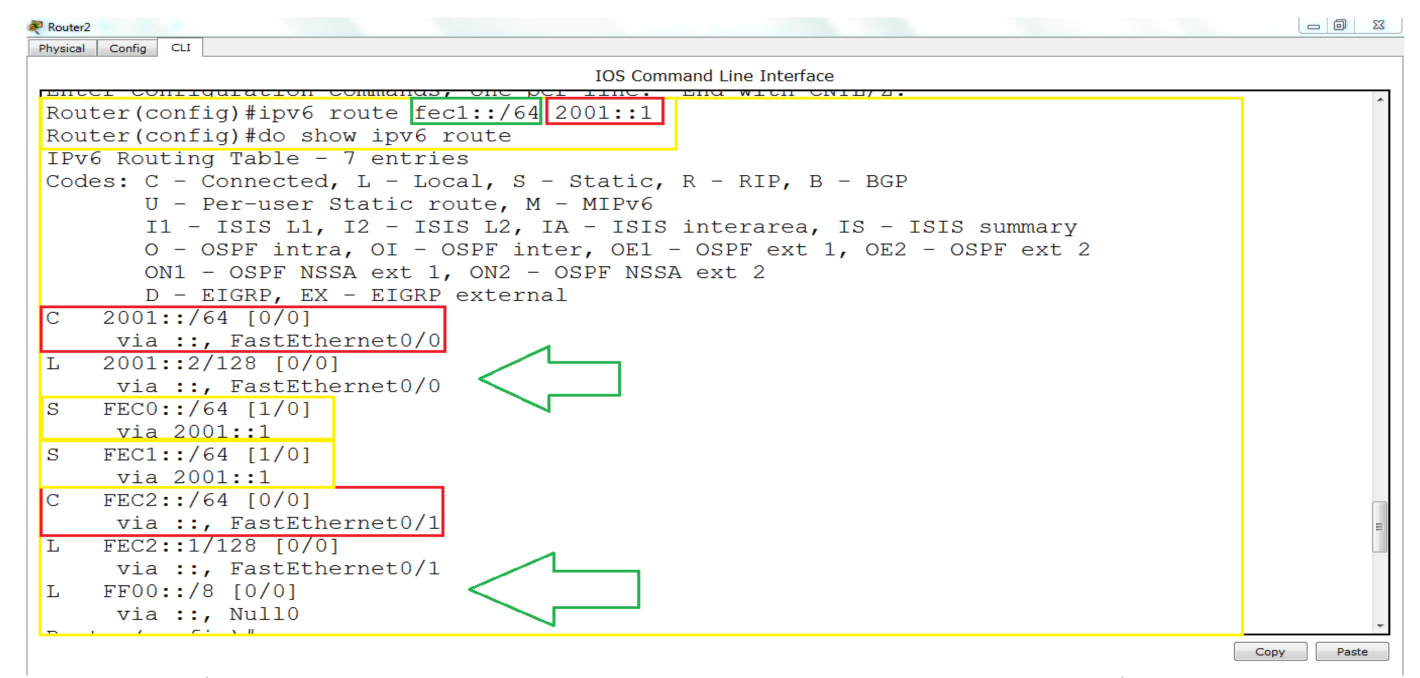
Router > **enable**

Router # **config t**

Router (config) **# ipv6 route fec1::/64 2001::1** هذه امر التوجيه اليدوي

Router (config) # **do show ipv6 route** لعرض جدول التوجيه

هذه إعدادات التوجيه اليدوي في الراوتر الثاني **R2** كما في الصورة التالية من داخل الراوتر الثاني **R2**:

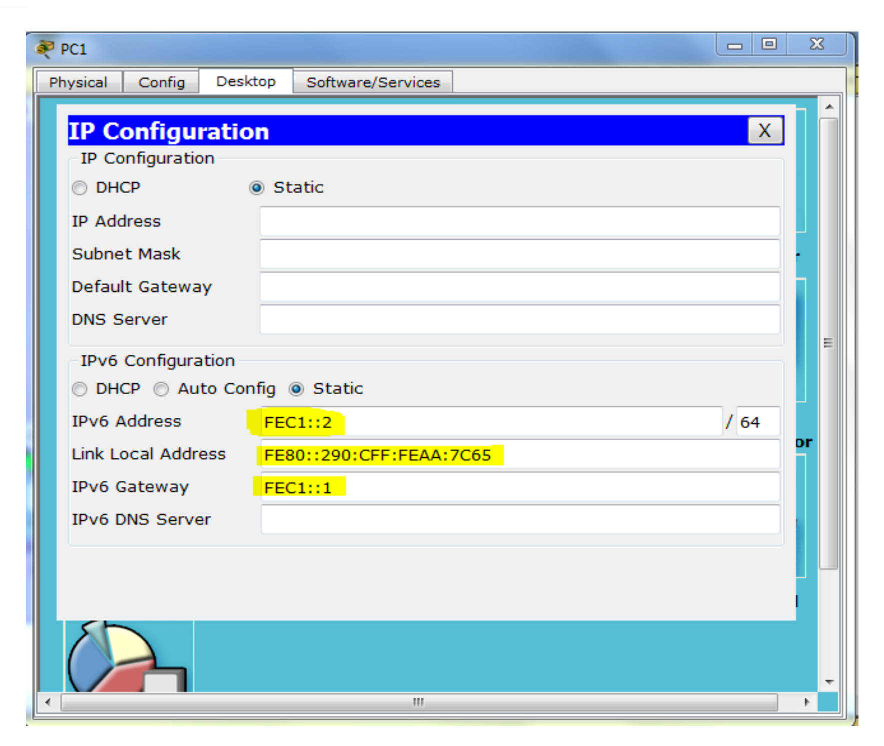


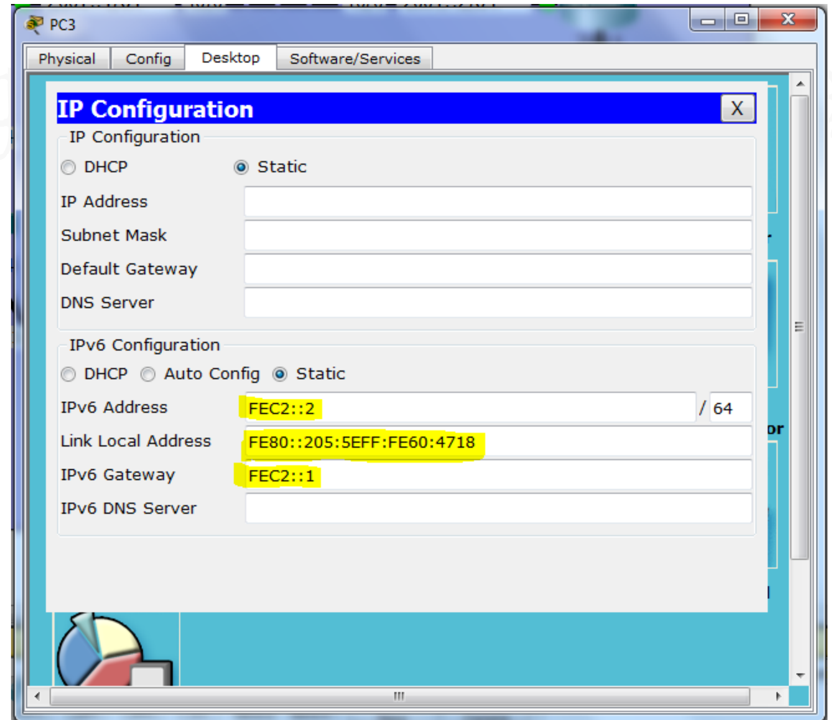
- لاحظ الأن بعد عرض جدول التوجيه سنجد الشبكة التي تم اضافتها في الراوتر الأول **R1** ولكن بشكل عكس ، بمعنى إنه الشبكات المتصلة مع الراوتر الثاني **R2** تستطيع الاتصال بشبكة المتصلة مع الراوتر الأول **R1** بهذه الطريقة جميع الشبكات تستطيع الاتصال مع بعضها البعض عن طريق التوجيه اليدوي ، و سنقوم الأن بعمل اختبار للشبكة هل متصلة مع بعضها البعض بشكل صحيح أو لا و سيتم الاختبار عن طريق أمر الـ **Ping** ما بين الشبكات التي تنفصل ما بينهم راوتر كما في الصورة التالية :
- هذا الاختبار **من R2** الى **R1** لاحظ إنه تم الرد بعلامة **!!!!!** هذا يدل على الاتصال بشكل صحيح .

```
Router#ping 2001::1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001::1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/1 ms
```

- و سيتم كتابة عنوان الـ **IPv6** في أجهزة الحاسوب في الشبكة بشكل التالي كما في الصورة :





- بهذا الشكل يكون قد تم الانتهاء من درس التوجيه اليدوي و التطبيق العملي على الشبكة والأن سنقوم بدخول على التوجيه الديناميكي الذي نقوم بتوجيه الشبكات عن طريق البروتوكولات مثل الـ **RIPng** , **OSPFv3** , **EIGRP** .

Dynamic Routing IPv6

Routing Information Protocol Next Generation (RIPng)

- **RIPng:** هو نفسه بروتوكول الـ **RIP** ولكن الـ **RIPng** مطور و يعتبر هو الإصدار الثالث لبروتوكول الـ **RIPng**، حيث إنه يتعمل مع عناوين الإصدار السادس و الشبكة التي تعمل في عنوان الإصدار السادس ايضاً، الـ **RIPng** يعمل مع **Port 521** و يستخدم بروتوكول الـ **UDP**، و يستخدم ايضاً رقم معالجة **Process ID** و يعمل على العنوان التالي **Multicast Group FF02::9** .

- **سنتعرف على إعدادات بروتوكول الـ RIPng :**

Router (config) # **ipv6 unicast-routing**

Router (config) # **ipv6 router rip 1** ← **Process ID**

Router (config-rtr) # **exit**

Router (config) # **interface fastethernet 0/0**

Router (config-if) # **ipv6 rip 1 enable**

Router (config-if) # **exit**

Router (config) # **show ipv6 router** ← **لعرض جدول التوجيه**

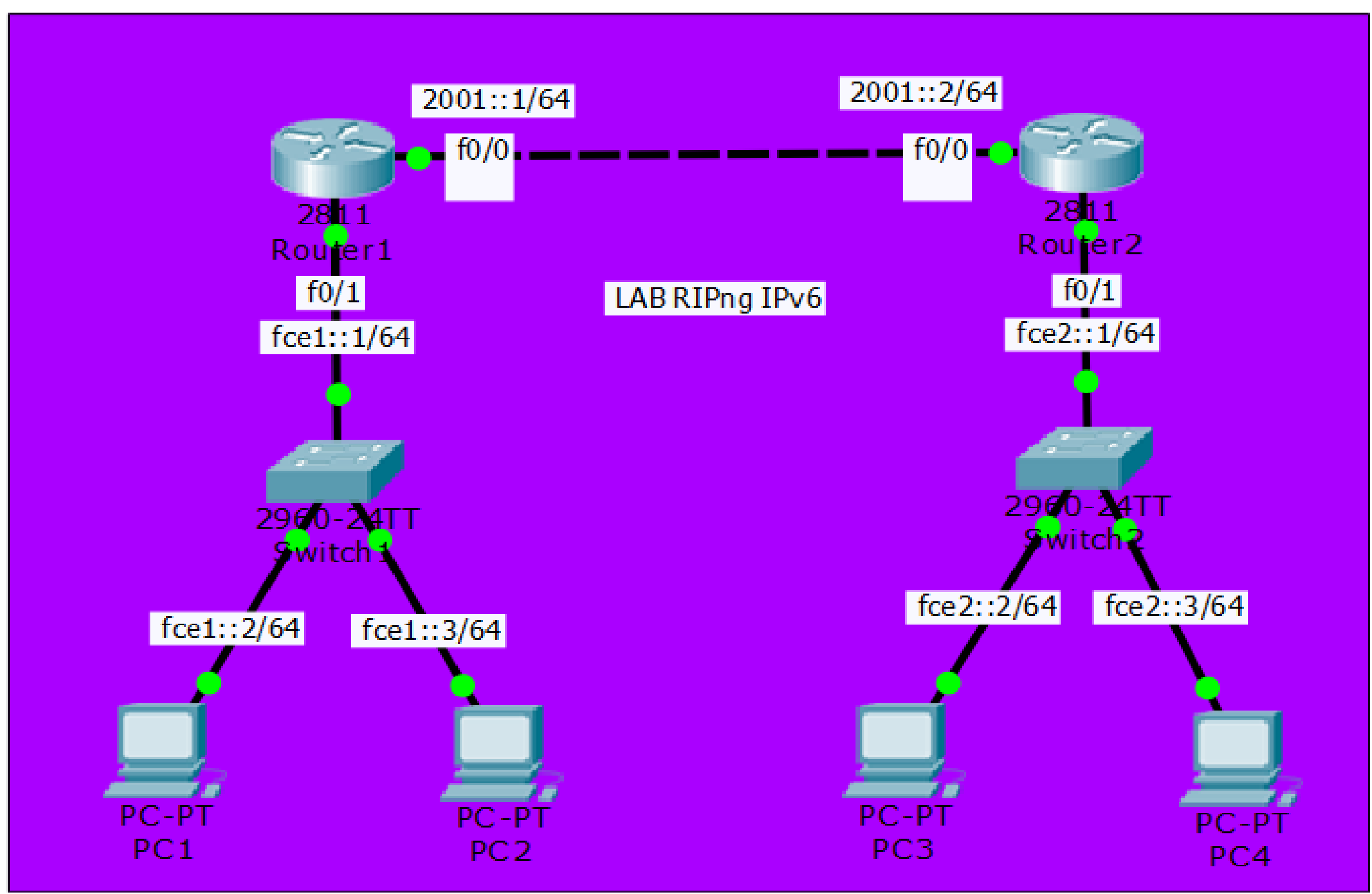
- ملاحظة مهم جداً قبل أن نقوم بتطبيق العملي بروتوكول الـ **RIPng** ، يعتمد اعتماد كبير على رقم العملية و هو الـ **Process ID** إذا اختلف الـ **Process ID** في الشبكة في هذه الحالة لا تستطيع الشبكات أن تتصل مع بعضها البعض .

- **الإعدادات التي سيتم بناء الشبكة عليها .**
- **في البداية يجب معرفة الإعدادات التي سيتم العمل عليها و معرفة الشبكات الـ 3 :**

١. الشبكة الأولى ستكون بعنوان **fec1::1/64**
٢. الشبكة الثانية ستكون بعنوان **fec2::1/64**
٣. الشبكة الثالثة ستكون بعنوان **2001::1 /64**

هذه إعدادات الشبكة كلها ويجب أن نعلم أن الشبكة الثالثة هي التي سترتبط ما بين الشبكة الأولى و الثاني ، ليتم الاتصال فيما بينهم بعد أن نقوم بعملية التوجيه .

الأن بعد أن تعرفنا على الشبكات و الإعدادات سنقوم بعمل إعدادات و تشغيل الإنترفيس و تركيب الاي بي على جميع الإنترفيس الموجودة على الراوترات و بعده سنقوم بعمل إعدادات بروتوكول الـ **RIPng** لبناء جدول التوجيه و إضافة الشبكات في الراوتر ، لتسطيع جميع



الشبكات الاتصال مع بعضها البعض مثل ما في النموذج التالي المرفق .

النموذج التالي هو الذي سيتم العمل عليه

- **الأن سنقوم بدخول على الراوتر الأول R1 و نقوم بكتابة الإعدادات التالية :**

سنقوم بكتابة الاومر التالية :

Router> **enable**

Router # **config t**

Router (config) # **ipv6 unicast-routing**

Router (config) # **ipv6 router rip 1**

Router (config-rtr) # **exit**

Router (config) # **interface fastethernet 0/0**

Router (config-if) # **ipv6 address 2001::1/64**

Router (config-if) # **ipv6 rip 1 enable**

Router (config-if) # **no shutdown**

Router (config-if) # **exit**

Router (config) # **interface fastethernet 0/1**

Router (config-if) # **ipv6 address fec1::1/64**

Router (config-if) # **ipv6 rip 1 enable**

Router (config-if) # **no shutdown**

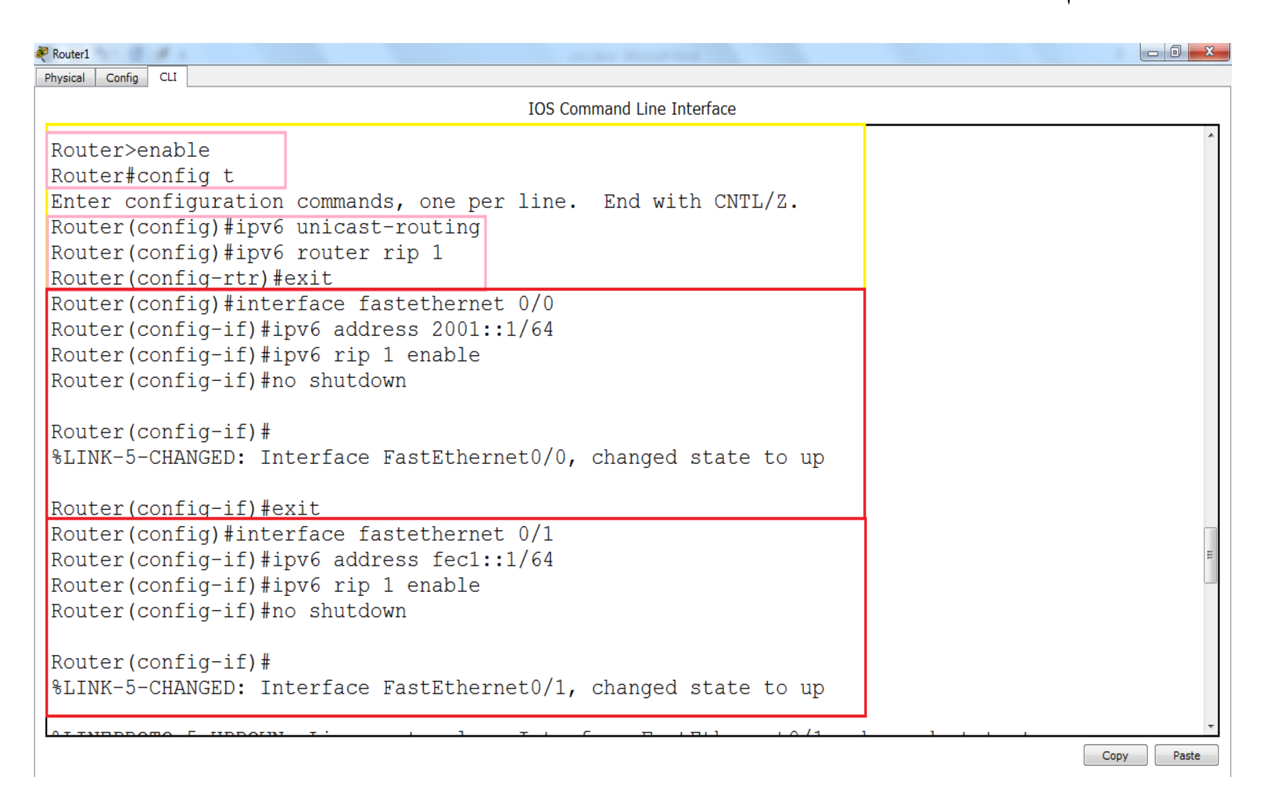
Router (config-if) # **end**

Router # **copy running-config startup-config**

-هذه إعدادات الراوتر الأول، مع العلم لقد قمنا ايضاً بتفعيل بروتوكول الـ **RIPng**، كما في الصورة التالية من داخل **R1**:

- **الأن سنقوم بدخول على الراوتر الثاني R2 و نقوم بكتابة الإعدادات التالية :**

سنقوم بكتابة الاوامر التالية :



```
Router> enable
Router # config t
Router (config) # ipv6 unicast-routing
Router (config) # ipv6 router rip 1
Router (config-rtr) # exit
Router (config) # interface fastethernet 0/0
Router (config-if) # ipv6 address 2002::1/64
Router (config-if) # ipv6 rip 1 enable
Router (config-if) # no shutdown
Router (config-if) # exit
Router (config) # interface fastethernet 0/1
Router (config-if) # ipv6 address fec2::1/64
Router (config-if) # ipv6 rip 1 enable
Router (config-if) # no shutdown
Router (config-if) # end
Router # copy running-config startup-config
```


- هذه إعدادات الراوتر الثاني، مع العلم لقد قمنا ايضاً بتفعيل بروتوكول الـ **RIPng**، كما في الصورة التالية من داخل **R2**:

Router2

Physical | Config | CLI

IOS Command Line Interface

```
Router>enable
Router#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#ipv6 unicast-routing
Router(config)#ipv6 router rip 1
Router(config-rtr)#exit
Router(config)#interface fastethernet 0/0
Router(config-if)#ipv6 address 2001::2/64
Router(config-if)#ipv6 rip 1 enable
Router(config-if)#no shutdown

Router(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up

Router(config-if)#exit
Router(config)#interface fastethernet 0/1
Router(config-if)#ipv6 address fec2::1/64
Router(config-if)#ipv6 rip 1 enable
Router(config-if)#no shutdown

Router(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to up
```

Copy | Paste

- الأن قمنا بعمل إعدادات بروتوكول الـ **RIPng** على الراوترات و تم إضافة الشبكات في جداول التوجيه الخاص في الراوترات ، ولكن نريد أن نقوم بعرض جداول التوجيه للراوتر لنتاكد من إنه تم إضافة الشبكات في جدول التوجيه أو لا سنقوم بدخول على الراوتر الأول **R1** و نقوم بكتابة الأمر التالي الخاص في عرض جدول التوجيه :

Router (config) # **show ipv6 route**

```
IPv6 Routing Table - 6 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user Static route, M - MIPv6
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
       D - EIGRP, EX - EIGRP external
C   2001::/64 [0/0]
     via ::, FastEthernet0/0
L   2001::1/128 [0/0]
     via ::, FastEthernet0/0
C   FEC1::/64 [0/0]
     via ::, FastEthernet0/1
L   FEC1::1/128 [0/0]
     via ::, FastEthernet0/1
R   FEC2::/64 [120/2]
     via FE80::260:2FFF:FE02:3E01, FastEthernet0/0
L   FF00::/8 [0/0]
     via ::, Null0
```

- كما نلاحظ من داخل الراوتر الأول **R1** إنه يوجد عدة شبكات ، و يوجد الشبكة التي تعمل تفعيل بروتوكول الـ **RIPng** و اختصار البروتوكول برمز **R** و قيمة المسافة الاداري [**120/2**] التي تم شرحه في الدروس السابقة .

- سنقوم بدخول على الراوتر الثاني **R2** ايضاً لنتاكد هل تم إضافة الشبكة المفعل عليه بروتوكول الـ **RIPng** أو لا .

Router (config) # **show ipv6 route**

```
IPv6 Routing Table - 6 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user Static route, M - MIPv6
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
       D - EIGRP, EX - EIGRP external
C   2001::/64 [0/0]
     via ::, FastEthernet0/0
L   2001::2/128 [0/0]
     via ::, FastEthernet0/0
R   FEC1::/64 [120/2]
     via FE80::240:BFF:FE56:D601, FastEthernet0/0
C   FEC2::/64 [0/0]
     via ::, FastEthernet0/1
L   FEC2::1/128 [0/0]
     via ::, FastEthernet0/1
L   FF00::/8 [0/0]
     via ::, Null0
```

- كما نلاحظ من داخل الراوتر الثاني **R2** إنه يوجد عدة شبكات ، و يوجد الشبكة التي تعمل تفعيل بروتوكول الـ **RIPng** و اختصار البروتوكول برمز **R** .

Opne Shortest Path First (OSPFv3)

OSPFv3: هو تطوير من بروتوكول الـ **OSPF** الذي كان يعمل مع العناوين من الإصدار الرابع، اما الأن لقد تم تطوير بروتوكول الـ **OSPF** الى **OSPFv3** ليتسطيع أن يعمل مع العناوين من الإصدار السادس و تم إضافة بعض الخصائص على هذه البروتوكول مثل الـ **IPsec** و التوثيق **Authentication** و التشفير **Encryption** ، و تم تغير عنوان البث المتعدد الخاص فيه ليكون **FF02::6** / **FF02::5** هذه عناون البث المتعدد الخاص في بروتوكول الـ **OSPFv3** الذي كان في بروتوكول الـ **OSPF** القديم الذي كان يعمل مع عنوان الإصدار الرابع و كان عنوان البث المتعدد الخاص فيه **224.0.0.6** / **224.0.0.5**.

- **سنتعرف على إعدادات بروتوكول الـ OSPFv3 :**

Router (config) # **ipv6 unicast-routing**

Router (config) # **ipv6 router ospf 1** ← **Process ID**

Router (config-rtr) # **router-id 200.200.200.200**

Router (config-rtr) # **exit**

Router (config) # **interface fastethernet 0/0**

Router (config-if) # **ipv6 ospf 1 area 0**

Router (config-if) # **exit**

Router (config) # **show ipv6 route**

- ملاحظة مهم جداً قبل أن نقوم بتطبيق العملي بروتوكول الـ **OSPFv3** ، هذا البروتوكول يعتمد على رقم العملية الـ **Process ID** و يعتمد ايضاً على رقم المنطقة الـ **Area ID** لتعمل الشبكة بشكل صحيح و اذا تم اختلاف هذه الإعدادات عن بعض لان تعمل الشبكة ولا تستطيع الاتصال مع بعضهم البعض .

- **الإعدادات التي سيتم بناء الشبكة عليها .**

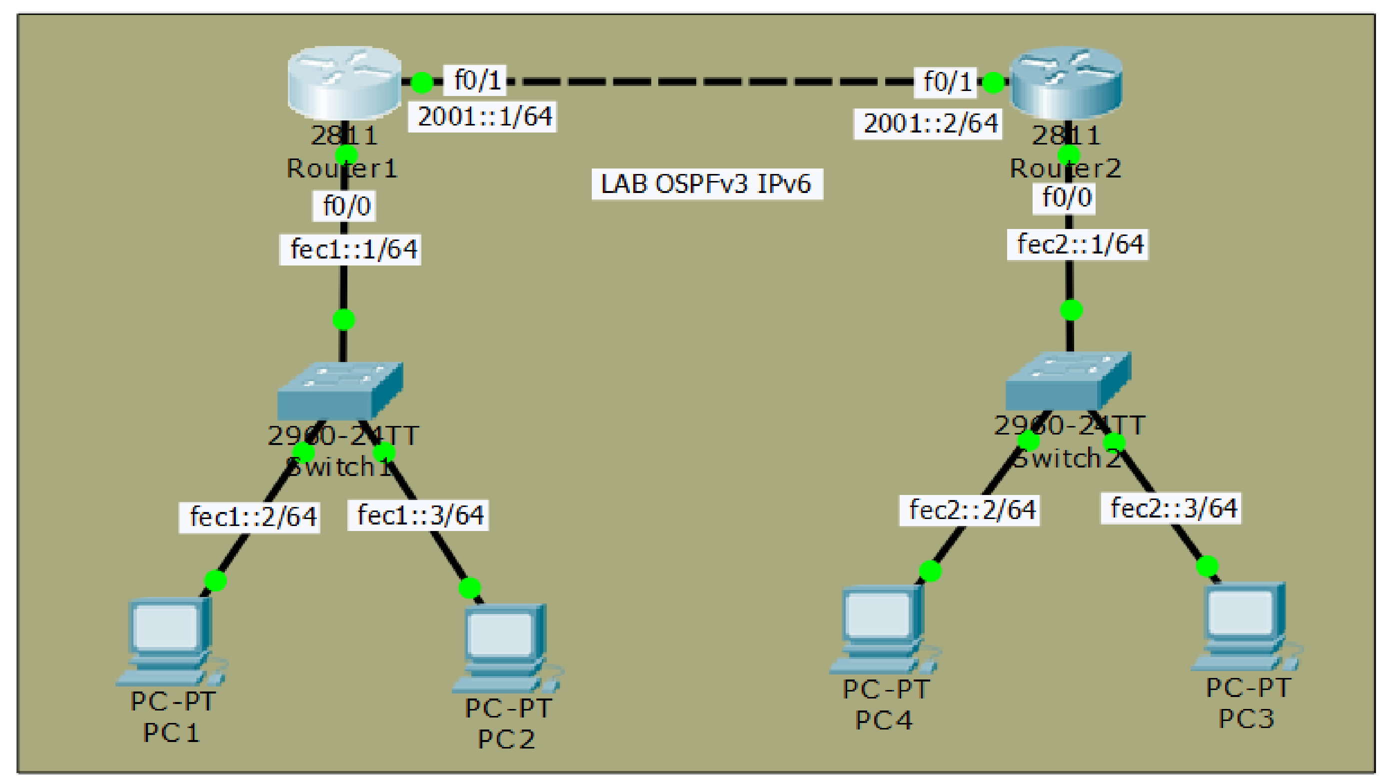
- **في البداية يجب معرفة الإعدادات التي سيتم العمل عليها و معرفة الشبكات الـ 3 :**

١. الشبكة الأولى ستكون بعنوان **fec1::1/64**
٢. الشبكة الثانية ستكون بعنوان **fec2::1/64**
٣. الشبكة الثالثة ستكون بعنوان **2001::1 /64**

هذه إعدادات الشبكة كلها ويجب أن نعلم أن الشبكة الثالثة هي التي سترتبط ما بين الشبكة الأولى و الثاني ، ليتم الاتصال فيما بينهم بعد أن نقوم بعملية التوجيه .

الأن بعد أن تعرفنا على الشبكات و الإعدادات سنقوم بعمل إعدادات و تشغيل الإنترفيس و تركيب الاي بي على جميع الإنترفيس الموجودة على الراوترات و بعدها سنقوم بعمل إعدادات بروتوكول الـ **OSPFv3** لبناء جدول التوجيه و إضافة الشبكات في الراوتر ، لتستطيع جميع الشبكات الاتصال مع بعضها البعض مثل ما في النموذج التالي المرفق .

النموذج التالي هو الذي سيتم العمل عليه



- **الأن سنقوم بدخول على الراوتر الأول R1 و نقوم بكتابة الإعدادات التالية :**

سنقوم بكتابة الاومر التالية :

Router> **enable**

Router # **config t**

Router (config) # **ipv6 unicast-routing**

Router (config) # **ipv6 router ospf 1**

Router (config-rtr) # **router-id 100.100.100.100**

Router (config-rtr) # **exit**

Router (config) # **interface fastethernet 0/1**

Router (config-if) # **ipv6 address 2001::1/64**

Router (config-if) # **ipv6 ospf 1 area 0**

Router (config-if) # **no shutdown**

Router (config-if) # **exit**

Router (config) # **interface fastethernet 0/0**

Router (config-if) # **ipv6 address fec1::1/64**

Router (config-if) # **ipv6 ospf 1 area 0**

Router (config-if) # **no shutdown**

Router (config-if) # **end**

Router # **copy running-config startup-config**

-هذه إعدادات الراوتر الأول، مع العلم لقد قمنا ايضاً بتفعيل بروتوكول الـ **OSPFv3**.

- **الأن سنقوم بدخول على الراوتر الثاني R2 و نقوم بكتابة الإعدادات التالية :**

سنقوم بكتابة الاومر التالية :

Router> **enable**

Router # **config t**

Router (config) # **ipv6 unicast-routing**

Router (config) # **ipv6 router ospf 1**

Router (config-rtr) # **router-id 200.200.200.200**

Router (config-rtr) # **exit**

Router (config) # **interface fastethernet 0/1**

Router (config-if) # **ipv6 address 2001::2/64**

Router (config-if) # **ipv6 ospf 1 area 0**

Router (config-if) # **no shutdown**

Router (config-if) # **exit**

Router (config) # **interface fastethernet 0/0**

Router (config-if) # **ipv6 address fec2::1/64**

Router (config-if) # **ipv6 ospf 1 area 0**

Router (config-if) # **no shutdown**

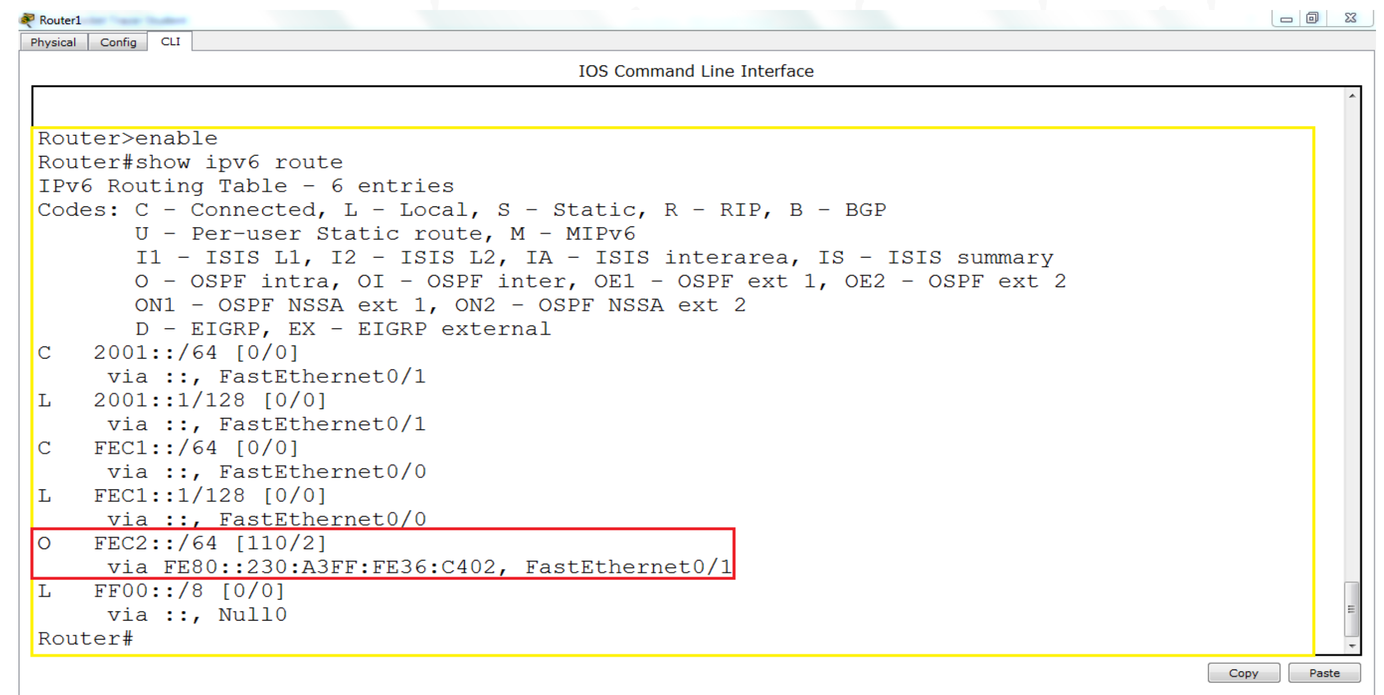
Router (config-if) # **end**

Router # **copy running-config startup-config**

- الأن قمنا بعمل إعدادات بروتوكول الـ **OSPFv3** على الراوترات و تم إضافة الشبكات في جداول التوجيه الخاص في الراوترات ، ولكن نريد أن نقوم بعرض جداول التوجيه للراوتر لنتاكد من إنه تم إضافة الشبكات في جدول التوجيه أو لا سنقوم بدخول على الراوتر الأول **R1** و نقوم بكتابة الأمر التالي الخاص في عرض جدول التوجيه :

Router (config) # **show ipv6 route**

R1

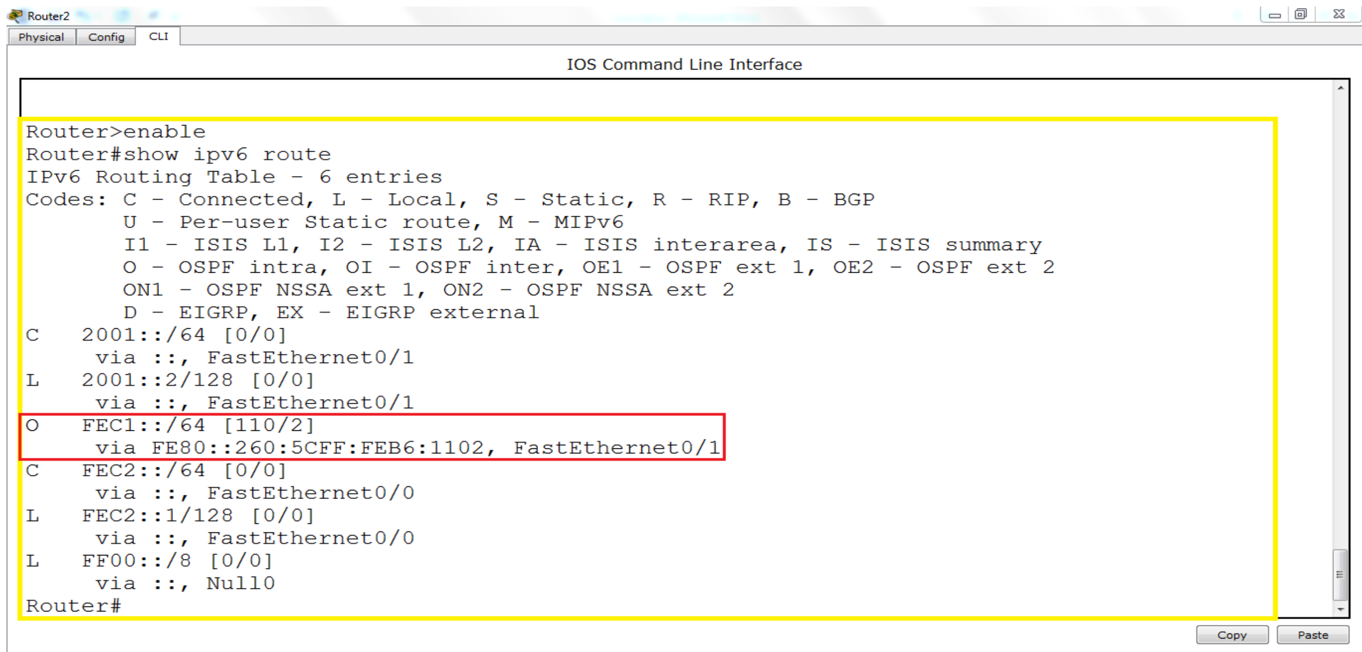


- كما نلاحظ من داخل الراوتر الأول **R1** إنه يوجد عدة شبكات ، و يوجد الشبكة التي تعمل تفعيل بروتوكول الـ **OSPFv3** و إختصار البروتوكول برمز **O** و قيمة المسافة الادارى [**110/2**] التي تم شرحه في الدروس السابقة .

- سنقوم بدخول على الراوتر الثاني **R2** ايضاً لنتاكد هل تم إضافة الشبكة المفعلة عليها بروتوكول الـ **OSPFv3** أو لا .

Router (config) # **show ipv6 route**

R2



```
Router>enable
Router#show ipv6 route
IPv6 Routing Table - 6 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user Static route, M - MIPv6
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
       D - EIGRP, EX - EIGRP external
C   2001::/64 [0/0]
     via ::, FastEthernet0/1
L   2001::2/128 [0/0]
     via ::, FastEthernet0/1
O   FEC1::/64 [110/2]
     via FE80::260:5CFF:FEB6:1102, FastEthernet0/1
C   FEC2::/64 [0/0]
     via ::, FastEthernet0/0
L   FEC2::1/128 [0/0]
     via ::, FastEthernet0/0
L   FF00::/8 [0/0]
     via ::, Null0
Router#
```

- كما نلاحظ من داخل الراوتر الثاني **R2** إنه يوجد عدة شبكات ، و يوجد الشبكة التي تعمل تفعيل بروتوكول الـ **OSPFv3** و اختصار البروتوكول برمز **O** .

- سنتعرف الأن بعد عملية الإعدادات من الراوتر الرائيسي و الراوتر الاحتياطي سنقوم بكتابة الأمر التالي في الراوتر الأول **R1** , Router # show ipv6 ospf neighbor

R1

```
Router#show ipv6 ospf neighbor

Neighbor ID      Pri   State      Dead Time   Interface ID    Interface
200.200.200.200   1    FULL/DR    00:00:35    2               FastEthernet0/1
Router#
```

R1

- لاحظ إنه الراوتر الأول **R1** هو الذي نجح في عملية الانتخاب و اصبح **DR** ، وسنقوم بدخول للراوتر الثاني **R2** و نعرض ما هي المعلومات الذي يحتوي عليها .

R2

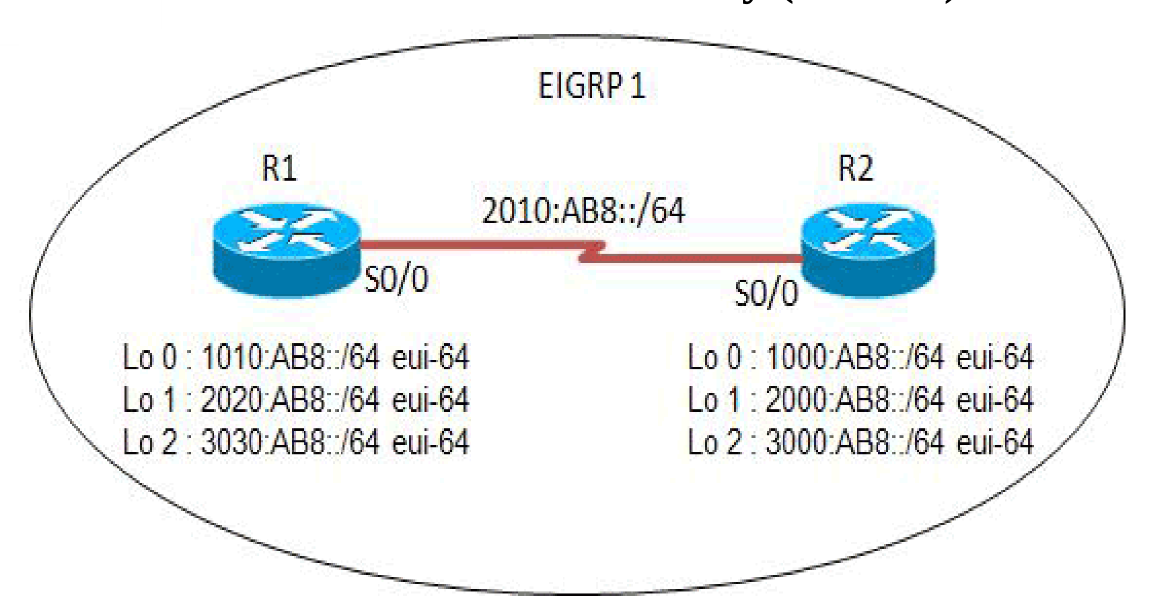
```
Router#show ipv6 ospf neighbor

Neighbor ID      Pri   State      Dead Time   Interface ID    Interface
100.100.100.100   1    FULL/BDR   00:00:38    2               FastEthernet0/1
Router#
```

لاحظ إنه الراوتر الثاني **R2** هو الذي سيكون الراوتر الاحتياطي BDR.

Router # show ipv6 ospf neighbor / Router # show ipv6 ospf database

Enhanced Interior Gateway (EIGRP)



EIGRP: هو بروتوكول مليكة خاصة بشركة سيسكو كما نعرف من الدروس السابقة و لقد قامت شركة سيسكو بتطوير هذا البروتوكول ليستطع أن يعمل مع عناوين الإصدار السادس **IPv6,** ويجب أن لا ننسى أنه يعمل على البوابة الداخلية للشبكة **Interior Gateway** و تم تغير عنوان البث المتعدد الخاص فيه الذي كان في عنوان الإصدار الرابع **224.0.0.10** و اصبح في العنوان السادس **FF02::A** و كما نعلم إنه يعمل بنظام الـ **Router-ID** و **AS**.

- سنتعرف على إعدادات بروتوكول الـ **OSPFv3** :

Router (config) # **ipv6 unicast-routing**

Router (config) # **ipv6 router eigrp 1** ← **Process ID**

Router (config-rtr) # **router-id 1.1.1.1**

Router (config-rtr) # **exit**

Router (config) # **interface fastethernet 0/0**

Router (config-if) # **ipv6 eigrp 1**

Router (config-if) # **end**

Router # **show ipv6 route**

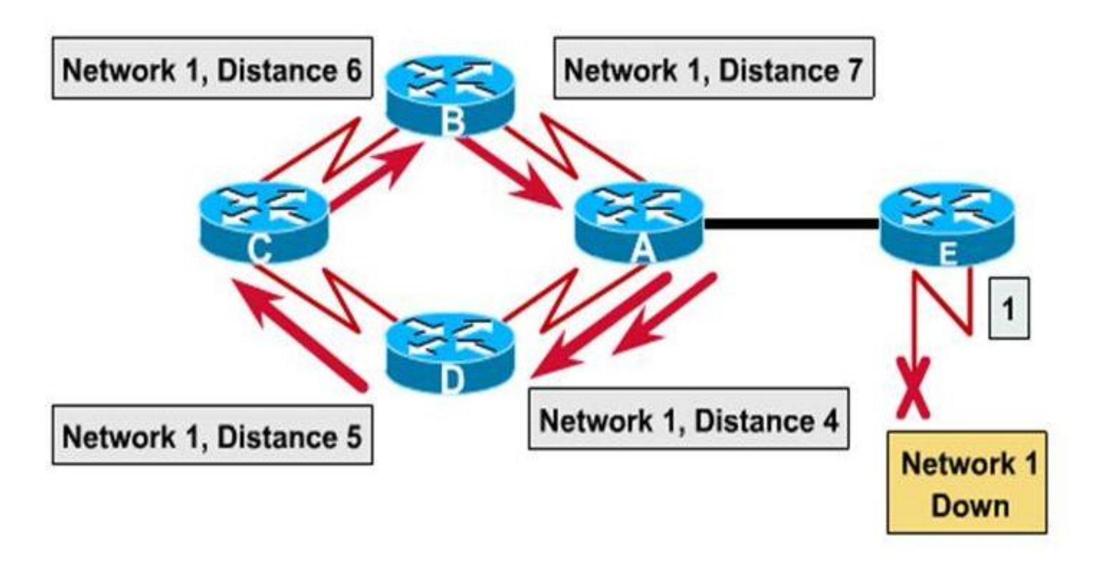
Router # **show ipv6 eigrp interfaces**

Router # **show ipv6 eigrp neighbors**

Router # **show ipv6 eigrp topology**

تقنيات منع دوران البيانات بين الموجهات

Routing Loops Avoidance



- تحدث مشكلة دوران البيانات في الشبكة عندما ا تريد شبكة الاتصال بشبكة أخرى وفي نفس الوقت تقوم الشبكة بإرسال و استقبال البيانات ، في هذه الحالة إذا حدث مشكلة في أحد الشبكات أو تم توقف راوتر ميعن في الشبكة ستبقى البيانات تقوم بعمل دوران في داخل الشبكة مما ينتج عن أختناق وازدحام في الشبكة وانشغال الشبكة أيضاً بشكل كبير جداً لن يتم ايقاف تشغيل الشبكة بشكل كامل ، ولكن يوجد عدة خدمات وعملية لمنع دوران البيانات في الشبكة سنتعرف عليها لنكون على معرفة و دراية كاملة ماذا يحدث في عملية دوران البيانات في الشبكة .

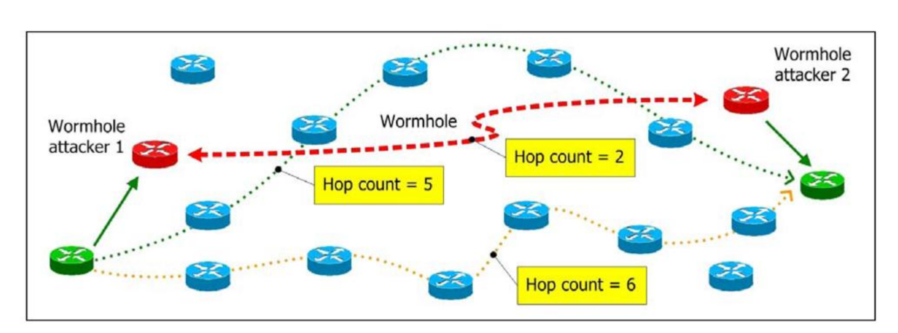
- يوجد خمسة أنواع من عملية منع دوران البيانات سنقوم بذكرها و شرحها لنفهم كل منهم ما هي وظيفتها ومتى يتم اختيارها :

1- Maximum Hop Count
2- Split Horizon
3- Route Poisoning
4- Hold Downs
5- Periodic Updates Triggered Updates

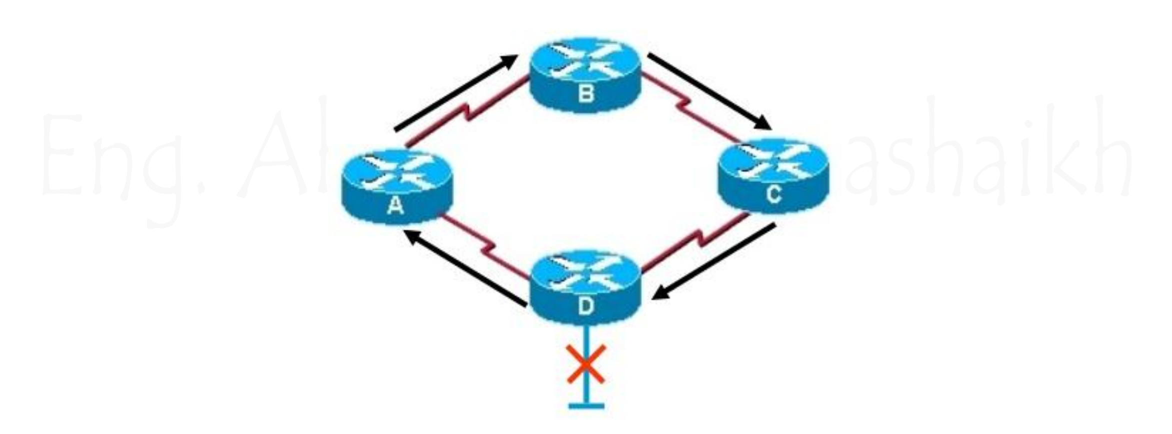
هذه هي الأنواع الخمسة الآن سنقوم بشرح كل واحد لوحده لنستطيع فهم هذه العملية .

ولكن قبل أن نبدأ في شرح هذه العملية والخاصية يجب أن نعرف كل بروتوكول من بروتوكولات التوجيه يستخدم أحد من هذه الخدمات في عملية منع دوران البيانات في الشبكة مثل يوجد بروتوكولات تستخدم نوعان من هذه العملية وبروتوكول آخر يستخدم عملية واحدة ، كل هذا يندرج تحت نوع البروتوكول المستخدم .

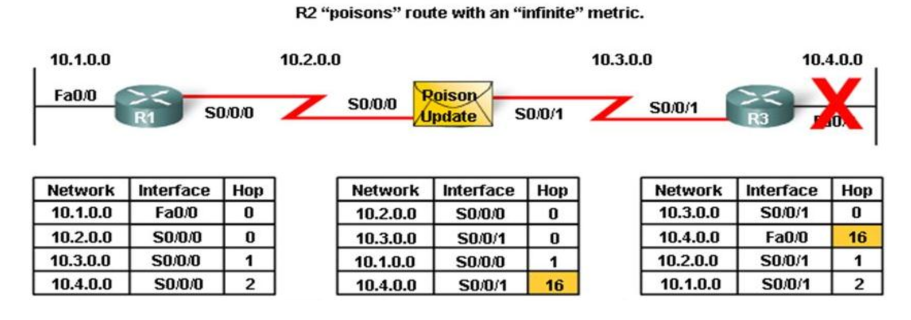
Maximum Hop Count : هذه العملية هي التي تحدد عدد القفزات ما بين الراوترت بمعنى كم هو عدد الراوترات الموجودة في المسار سيتم الاعتماد عليها أثناء عملية تنقل البيانات للوصول إلى أخرى نقطة وبعدها تنتهي البيانات ويتم إخراجها من الشبكة، و بروتوكولات التوجيه التي تعمل بهذه الخاصية بروتوكول الـ **EIGRP** , **RIP** هذه البروتوكولات التي تعمل بهذه الخدمة لمنع دوران البيانات.



Split Horizon : هذه العملية هي قاعدة عامة ومعروفة وتعمل بالطريقة التالية ، عندما ا يتم إرسال بيانات من جهة معينه لن تعود البيانات من الجهة التي أرسلت منها البيانات جميع بروتوكولات الشبكات تعمل بهذه القاعدة بشكل عام .



Route Poisoning: هذه العملية موجودة في بروتوكول الـ **RIP** ، ويعتبر بروتوكول الـ **RIP** بطيء في عملية التحديث حيث عندما ا يحدث تغير أو تعديل أو حذف أو تعديل سيتم أخذ بعض الوقت ليتم إرسال التحديثات لباقي الراوترات في الشبكة ، ولكن في حالة لم يصل التحديث و الراوتر لم يحصل على التحديث و الشبكة توقفة و الراوتر أصبح لديه علم أنه لم يستلم التحديث سيقوم بعمل عملية الـ **Route Poisoning** ويقوم بعمل الـ **Matric** آخر قيمة له تكون **16** فهذه هي نهاية الـ **Next Hop**.



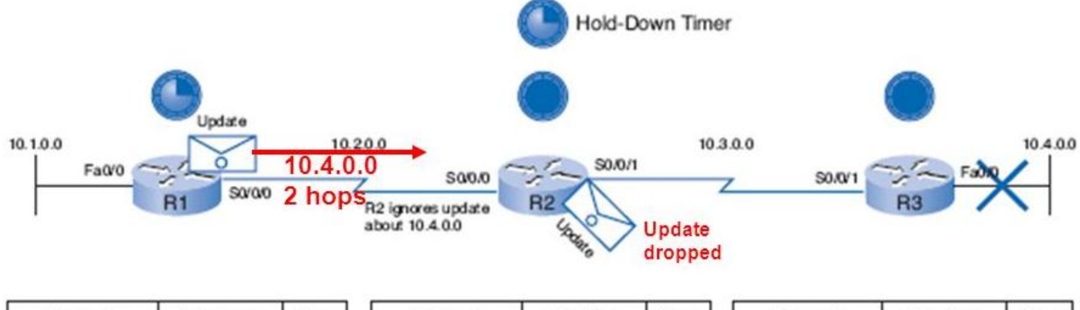
Network	Interface	Hop
10.1.0.0	Fa0/0	0
10.2.0.0	S0/0/0	0
10.3.0.0	S0/0/0	1
10.4.0.0	S0/0/0	2

Network	Interface	Hop
10.2.0.0	S0/0/0	0
10.3.0.0	S0/0/1	0
10.1.0.0	S0/0/0	1
10.4.0.0	S0/0/1	16

Network	Interface	Hop
10.3.0.0	S0/0/1	0
10.4.0.0	Fa0/0	16
10.2.0.0	S0/0/1	1
10.1.0.0	S0/0/1	2

Hold Downs: هذه العملية أيضاً موجودة في بروتوكول الـ **RIP** ، وهي عبارة عن قيمة زمانية **180** ثانية ووظيفتها الانتظار حتى أن يتم استلام تحديثات من الجيران وقتها سيتم إلغاء عملية قيمة التزامن الـ **180** ثانية ، أما إذا لم يستلم بعد مرور الوقت الزماني الـ **180** ثانية سيتم إلغاء الشبكات من جدول التوجيه .

Preventing Routing Loops with Hold-Down Timers



Network	Interface	Hop
10.1.0.0	Fa0/0	0
10.2.0.0	S0/0/0	0
10.3.0.0	S0/0/0	1
10.4.0.0	S0/0/0	2

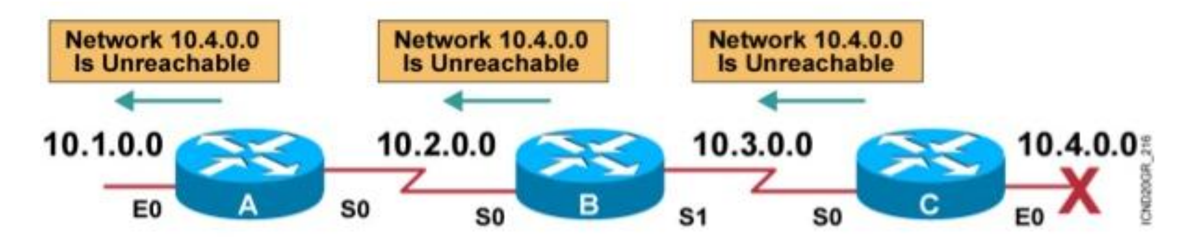
Network	Interface	Hop
10.2.0.0	S0/0/0	0
10.3.0.0	S0/0/1	0
10.1.0.0	S0/0/0	1
10.4.0.0	S0/0/1	1

Network	Interface	Hop
10.3.0.0	S0/0/1	0
~~10.4.0.0~~	~~S0/0/1~~	~~0~~
10.2.0.0	S0/0/1	1
10.1.0.0	S0/0/1	2

Same or worse metric received – Still possibly down - Keep Hold-down timer going

- If an update from any other neighbor is received during the hold-down period with the **same or worse metric** for that network, that update is ignored.
- Thus, more time is allowed for the information about the change to be propagated.

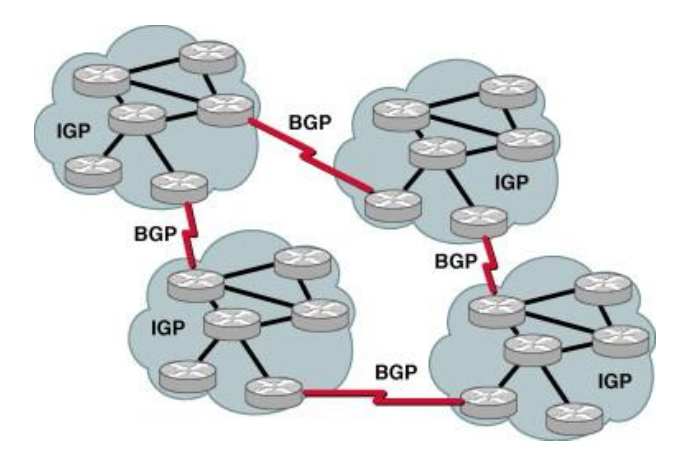
Periodic Updates Triggered Updates : هذه العملية عبارة عن تحديثات منفصله عن بعضهم البعض ، حيث يوجد التحديث الدوري والتحديث الفوري بينما الفرق بينهم أن التحديث الدوري يحدث في زمن معين مثلاً يتم ضبط وقت معين لعملية إرسال التحديثات في توقيت زماني محدد ، والتحديث الفوري هو عندما ا يحدث تحديث في نفس الوقت سيقوم بإرساله لجميع الراوترات الموجودة في الشبكة ليتم التعديل في جميع الراوترات الموجودة على الشبكة، بينما هذه العملية توفر للشبكة تخفيف كبير جداً من الضغط عليه وعدم انشغال الشبكة بشكل مستمر و يمنع استمرار دوران البيانات لأنه من المعروف أن التحديثات متوجهة لجهة معين بذاتها ولا يوجد داعي لعملية الدوران .



- **The router sends updates when a change in its routing table occurs.**

Border Gateway Protocol (BGP)

Baisics



BGP : هو عبارة عن بروتوكول مهم جداً جداً ويتم استخدامه في شبكات الانترنت بشكل كبير جداً ، ويعتمد عليه بشكل رسمي في ربط الشبكات الكبيرة والعملاقة بينما يقوم بربط الشبكات مع شبكات مزودي الخدمة **ISP** ليتم الاتصال بالشبكة الآخر التي تكون على مستوى العالم، هذا البروتوكول ضخم جداً ولديه مميزات كثيرة جداً ولكن لن نستطيع التعمق بشكل كبير جداً في دراسة وفهم هذا البروتوكول لأنه يوجد كورسات ودروس وكتب ضخمة لهذا البروتوكول في حال تريد التعمق فيها وتستطيع العمل عليها بشكل احترافي سنتعرف على البروتوكول الآن وماذا يدعم .

- كما نعلم أن البروتوكولات تنقسم إلى قسمين :

Interior gateway routing (IGP)

هذا النوع يندرج فيه البروتوكولات التي تعمل في الشبكات الداخلية مثل **OSPF** , **RIP** , **EIGRP**.

Exterior gateway routing (EGP)

هذا النوع يندرج فيه البروتوكولات التي تعمل بتوصيل الشبكات الداخلية مع الخارجية مثل يكون لدنيا شبكة في دولة ونحن نريد الاتصال بها، سيتم الربط عن طريق البروتوكولات التالية **EGP** , **BGP** وهذه البروتوكولات المسؤولة عن ربط الشبكات عن طريق الانترنت.

يعتمد بروتوكول الـ **BGP** في العمل على بروتوكول الـ **TCP** ويقوم بحجز البورت **179** ، ليستطيع الاتصال بباقي الراوترات التي تعمل بنفس البروتوكول .

- **سنتعرف على بعض التفاصيل ما قبل أن نتعمق في بروتوكول الـ BGP .**

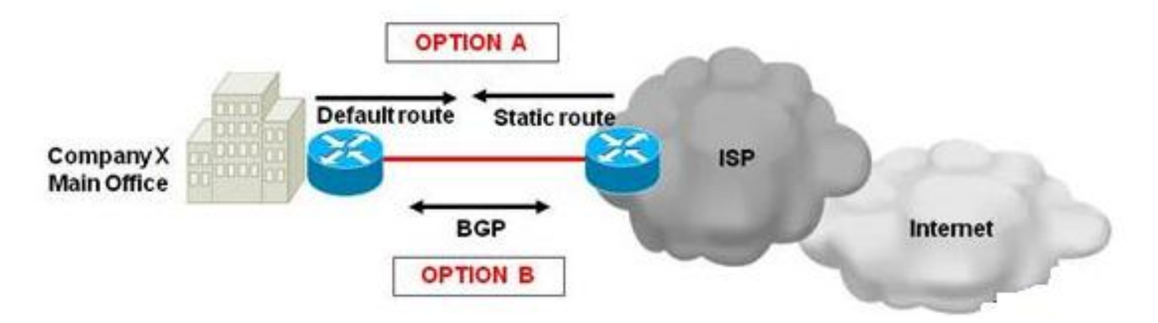
سنبدأ بالتعرف على بعض الخصائص التي يعمل فيها هذا البروتوكول لنستطيع أن نفهم ما هي الوظائف التي يعمل فيها البروتوكول .

- يعتبر بروتوكول الـ **BGP** من أهم البروتوكولات الموجودة في عالم الشبكة ويجب أن نكون على معرفة ولو بشكل بسيط في فهم ومعرفة المعلومات عنه .
- بروتوكول الـ **BGP** تم تطويره من بروتوكول سابق وهو **EGP** .
- يعتمد بروتوكول الـ **BGP** على خاصية تحديد المناطق وهي الـ **AS** الذي أيضاً يعتمد عليها بروتوكول الـ **EIGRP** .
- يعتبر هذا البروتوكول من أبطأ البروتوكولات الخاصة في التوجيه لأنه يربط الشبكات الكبيرة في بعضها البعض .
- يعمل بروتوكول الـ **BGP** على شكل **Path Vectory**.
يعمل في داخل بروتوكول نقل المعلومات والبيانات وهو الـ **TCP** في عملية الاتصال ما بين الراوترات الآخر .
- يتكون بروتوكول الـ**BGP** من ثلاث جداول **Peers Table , Topology Table Routing Table**.
- يتم حساب واعتماد اختيار أفضل مسار في بروتوكول الـ**BGP** عن طريق خوارزمية.
- عيب بروتوكول الـ **BGP** أنه يجب على مهندس الشبكة أن يقوم بعمل إعدادات تعريف وتوجيه الراوترات التي تعمل ببروتوكول الـ **BGP** بشكل يدوي .
- يحتوي على نوعان من البروتوكولات بروتوكول للشبكة الداخلية وبروتوكول للشبكة الخارجية .
بروتوكول الـ**BGP** هو بروتوكول غير محتقر بمعنى مفتوح المصدر.
- يتم استخدام بروتوكول الـ **BGP** على الأغلب بشكل كامل في شركة مزودي الخدمة.
- يعمل في الطبقة السابعة وهي طبقة الـ**Application** ويستخدم بروتوكول الـ **TCP Port 179** .
- يعمل بروتوكول الـ **BGP** على تبادل المعلومات والبيانات بشكل كامل في حالة أن الراوتر لم يسبق عليه تفعيل بروتوكول الـ**BGP** , وبعد تفعيل البروتوكول سيقوم بعمل إرسال كامل البيانات والمعلومات وبعدها يتوقف عن الإرسال وفي حال تم تحديث أو تم التعديل سيتم معاودة إرسال التحديثات .
- توقيت إرسال التحديثات عندما ا يتواجد تحديث في الراوتر، سيتم تجميع كل التحديثات وإرسالها دفعه واحدة وسيكون التوقيت للشبكات البعيدة أو الخارجية كل **30 Sec** ثانية وفي الشبكات الداخلية التي تخضع في داخل نطاق واحد AS سيكون توقيت التحديث كل **5 Sec** ثواني ، وهذه مفيدة في عدم انشغال الشبكة بشكل مستمر .
- تتم عملية تعريف الجيران بطريقة يدوية بمعنى أن مهندس الشبكة هو من يقوم بتعريف الجيران على الراوتر بجميع الراوترات الموجودة ، ولا يدعم الطريقة الديناميكية .
- قيمة المسافة الإدارية **Admin distance 20** في بروتوكول الـ**BGP Ex** الخارجي و في الداخلي **BGP In** تكون قيمة المسافة الادارية **Admin distance 200** .
- يعمل ويدعم تقسيم الشبكات **Classless , CIDR , Vlsm** .
- يعمل على منع دوران البيانات في الشبكة من خلال تقنية منع دوران البيانات وهي **Split-horizon** .

يوجد نوعان من الاتصال يتم استخدامها في بروتوكول الـ BGP :

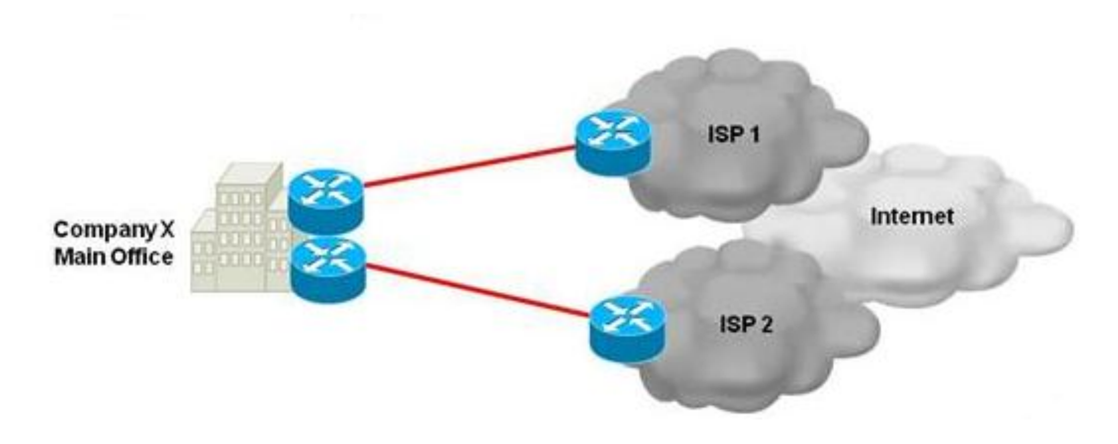
Single homed Customers

هذا النوع من الاتصال يكون متصل بشكل مباشر مع شركة مزودي الخدمة مثلاً عندما ا يكون شركة مزودي خدمة صغيرة فرع صغير منها ويتم ربطها بشركة مزودي خدمة عملاقة ويكون الاتصال مباشر .



Multi homed Coustomers

هذا النوع من الاتصال يكون أيضاً مباشر ولكن يكون متعدد مثلاً عندما ا يكون لدنيا شبكتين من مزودي الخدمة ومتصلين بهم من مكان واحد بمعنى نستطيع الاتصال بأي مزود نريد.



BGP Table , جداول الـ BGP

- يوجد ثلاث جداول يعتمد عليهم بروتوكول الـ **BGP** ويتم تبادلهم ما بين الراوترات التي تعمل ببروتوكول الـ **BGP** سنتعرف عليهم .

1- Neighbor Table

List of BGP Neighbors BGP peers, Configured statically

2- BGP forwarding database table

List of all Networks learned from each neighbor

3- IP routing table

List of best paths to destination networks

- سنقوم الأن بشرح الجداول لنتعرف عليها بشكل أفضل:

Neighbor Table: هذا الجدول يحتوي على قائمة كاملة بجميع الراوترات التي تعمل ببروتوكول الـ **BGP**.

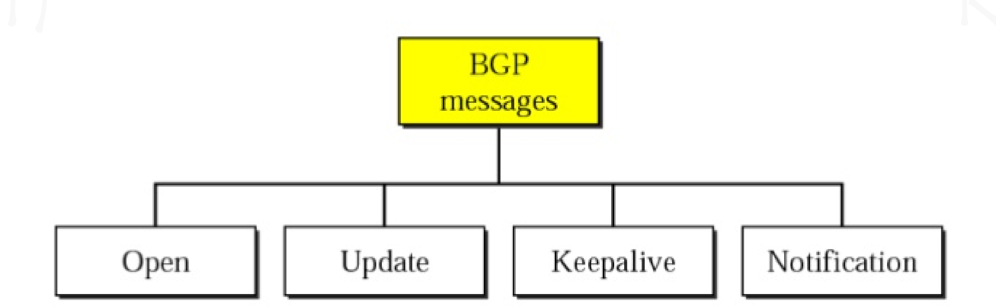
BGP forwarding database table: هذا الجدول الذي يحتوي على جميع المسارات والبيانات التي تم إرسالها واستقبالها ما بين الراوترات التي تعمل ببروتوكول الـ **BGP** حيث يتم تعرفة المسارات بشكل مفصل.

IP routing table: هذا الجدول يحتوي على جميع عناوين الشبكة التي تعمل ببروتوكول الـ **BGP**، ليستطيع أي من الشبكات المسجلهة في داخل الجدول من الوصول إلى الشبكات الآخر بكل سهولة.

BGP Messages

رسائل بروتوكول الـ BGP

- تستخدم هذه الرسائل في عملية التحديثات التي يستخدمها بروتوكول الـ **BGP** في عملية إرسال التحديثات، وكل رسالة لها وظيفتها الاساسية وتحتوي على معلومات سنقوم بشرح هذه الرسائل ، وتتكون من أربعة رسائل مهمة جداً :



1- Open Message
2- Notification Message
3- Update Message
4- Keepalive Message

هذه هي الرسائل المستخدمة في بروتوكول الـ **BGP** سنقوم بشرحها لنتعرف على ماذا تحتوي كل رسالة من المعلومات.

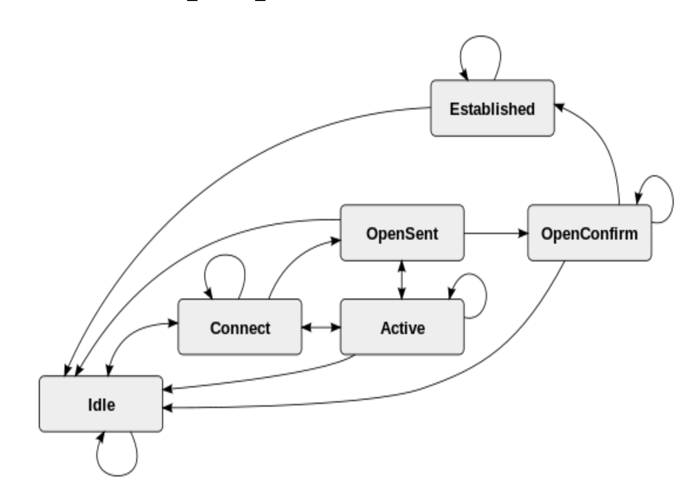
Open Message : هذه الرسالة المسؤولة عن تنظيم و فتح قناة اتصال ما بين الراوترات المجاورة، و تحتوي أيضاً على عنوان الـ **ID.**

Keepalive Message : هذه الرسالة المسؤولة عن تأكد قناة الاتصال مفتوحة أم لا ما بين الراوترات ليقوم بعملية الإرسال، ويتم إرسال رسالة تؤكد كل **60 Sec** ثانية لعملية التأكيد من أنه القناة مفتوحه أم لا.

Update Message: هذه الرسالة التي تحتوي على التحديثات مثل الشبكات الجديدة التي تم إضافتها والمسارات والكثير من التحديثات والمعلومات الآخر ى.

Notification Message: هذه الرسالة المسؤولة عن الأخطاء حيث تقوم بإرسال رسالة موجود بداخلها الأخطاء التي حصلت ليتم التعرف عليها وحلها.

حالة بداية تشغيل الـBGP , BGP Startup Operation



- عند عملية إعدادات وتفعيل بروتوكول الـ **BGP** على أحد الراوتر سيبدأ بتجهيز نفسه إلى عدة حالات ليبدأ في التغير والتحديث في الراوترات الآخر سنقوم بذكر الحالة وشرحها .

Idel State: هذه حالة الراوتر عندما ا نقوم بعملية البحث عن جدول التوجيه ليتعرف على الرواترات الآخر ى.

Active 1 State: هذه الرسالة في حالة لم يتم الرد بعد وقت معين سيتم تحويل الراوتر إلى هذه الحالة **Active**.

Connect State: هذه حالة الراوتر عندما ا يعرف الراوتر الرئيسي ويكون قد تم الإنتهاء من عملية التوثيق ما بينهم.

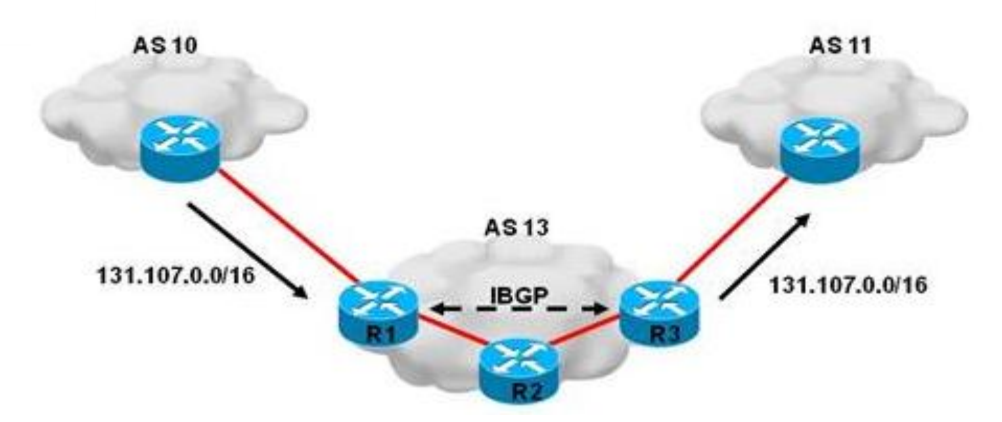
Open Sent: هذه رسالة يقوم بإرسالها الراوتر لمعرفة معلومات الجيران، ليستطيع ترتيب الاتصال ما بينهم.

Active 2 State: هذه الرسالة تقوم بعملية حسب قناة الاتصال ما قبل أن يقوم الراوتر بعملية الإرسال.

Open Confirm: هذه عبارة عن رسالة موافقة من الراوترات الآخر الموجودة في الشبكة للتأكد على موافقة فتح قناة الاتصال وتبادل المعلومات.

Established State: هذه الرسالة الاخيرة و هي عملية تبادل المعلومات ما بين الراوترات.

BGP Synchronization



- **Synchronization:** هي قاعدة في بروتوكول الـ **BGP** و وظيفة هذه القاعدة أنه لا نستطيع إرسال أي قاعدة **Rule** تم التعرف عليها من خلال الـ **IBGP** ، إلا إذا كان الراوتر متواجد في الـ **IGP** الخاصة في الشبكة الداخلية وتكون هذه القاعدة مفعله بشكل تلقائي ويجب على مهندس الشبكة عمل ايقاف لهذه العملية .

الأمر التالي هو الذي سنقوم بعمله لنقوم بعملية ايقاف العملية الـ Synchronization

Router (Config-Router) # no synchronization

Disables BGP Synchronization so a router can advertise routers in BGP without lerning them in IGP , but make sure that you make all restrictiong to avoid black holes .

- **BGP Split horizone rule : Avoid routing loops inside the AS**

هذه العملية مهمة جداً ووظيفتها كتالي عندما ا يقوم أحد الراوترات بإرسال تحديثات للجيران سيتم وصول التحديثات لكل الراوترات ويحصل بما يسمى **Loops** ولكن مع هذه العملية ستقوم بعمل بلوك على المنفذ الذي خرج منه التحديثات مثل عندما ا يقوم الراوتر بإرسال التحديث المنفذ لا يعاود استقبالها مرة أخرى لأنه تم الخروج منها ، و بهذه الحالة سيتمتجاوز عملية دوران البيانات في الشبكة **Loops Network**.

Full Mesh Fashion (sessions between all BGP neighbors) to avoid split horizon rule.

Full Mesh Fashion : عيب هذه الشبكة لو كان لدنيا شبكة مزود خدمة ضخمة جداً وجميع الراوترات متصلة مع بعضها البعض بشكل مباشر ، هذا عيب كبير جداً في استهلاك السرعة واستهلاك قوة الراوترات بشكل رهيب واشغال القطع المادية في داخل الراوترات أيضاً والشبكة ولكن يوجد بعض الحلول التي سنتعرف عليها :

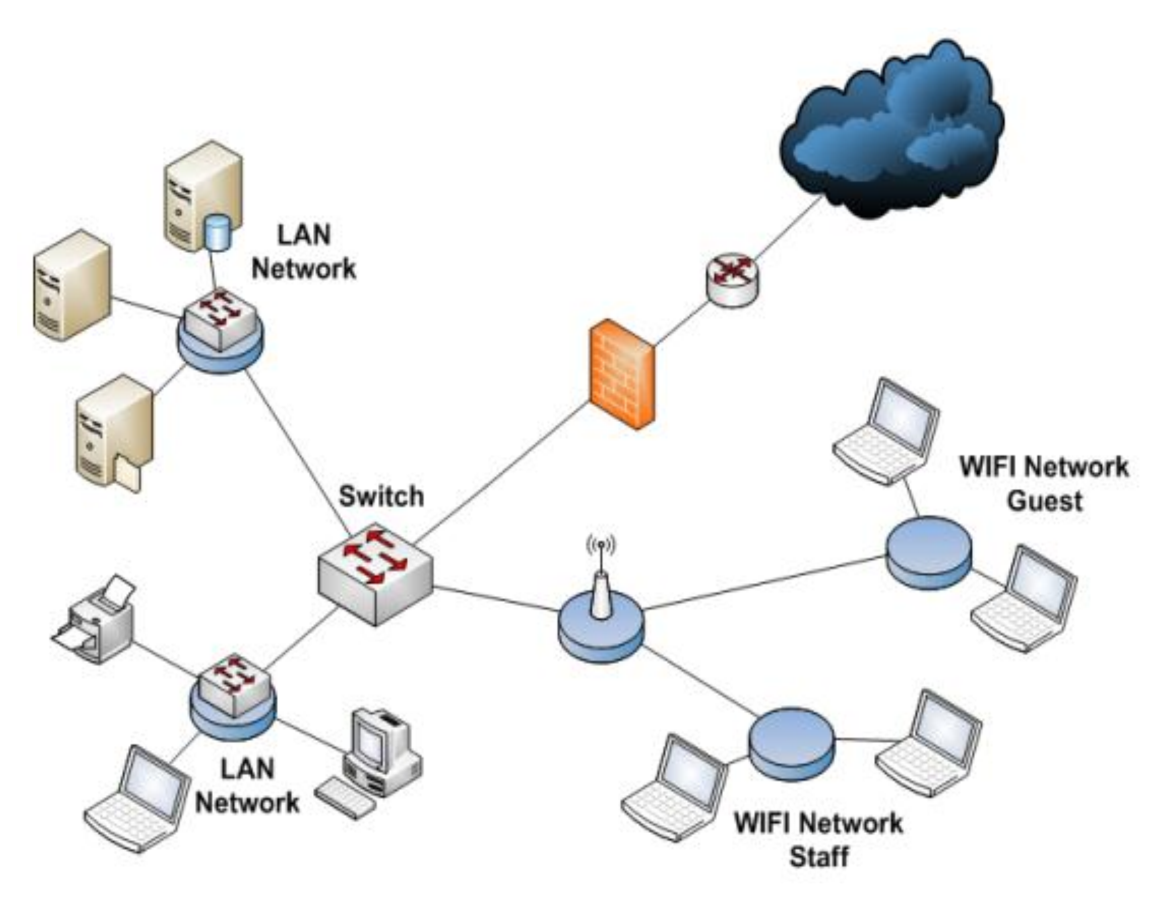
١- تقسيم الـ **AS** الى عدة **AS** مما يجعل الشبكة أكثر مرونة من أن تكون في **AS** واحد.
٢- **Route reflector** هذه العملية تقوم بوظيفة إلغاء عملية دوران البيانات بشكل نهائي.

فهرس المستوى الثالث

Ethernet LANs and Switches شبكات الإيثرنت المحلية و المبدل

Ethernet LANs
شبكات الإيثرنت المحلية

الشبكات المحلية LAN = Local Area Network: هي شبكات تستخدم لتغطية أماكن محدودة وصغيرة مثل المنزل أو المكتب أو شبكة داخلية كبير ولكن تحتاج لخوادم و معدات مثل السويتشات و الراوترات و الأجهزة .



هناك طريقتان لتوصيل الشبكات المحلية : إيثرنت **Ethernet** وتوكن رينغ **Token Ring** عند توصيل الحواسيب بطريقة الايثرنت فإنها يتم توصيلها بالعادة إلى مجمع أو مبدل بمعنى السويتش .

يمكن توصيل الشبكات المحلية مع بعضها عن طريق موصلات من الشبكات الواسعة **WAN** ، وذلك باستخدام الموجهات **Router** .

فوائد الشبكات المحلية :

تسهيل تبادل الملفات بين الأجهزة في نفس الشبكة المحلية لأجل توفير الوقت المستغرق لنقل الملفات، فتعتبر الشبكة المحلية عامل توفير اقتصادي في الشبكات حيث لا تحتاج في كل مكتب إلى جهاز طابعة ومن الممكن توصيل كل الأجهزة الحاسوب في الشركة أو المكتب إلى طابعة واحدة أو ماسحة ضوئية واحدة أو غيرها من الآلات والأجهزة الحاسوبية.

الايثرنت **Ethernet** : تعبر الإيثرنت عن مجموعة قواعد عامة لتوصيف طريقة الربط الفيزيائي ونقل رسائل المعطيات (**frames**) بين مجموعة محطات عمل (**workstations**) في الـ الشبكة المحلية (**LANs**) وتعتبر تمثيلاً للطبقتين **1** الطبقة الفيزيائية **physical layer** و **2** طبقة ربط المعطيات **data link layer** في توصيف اتصال النظم المفتوحة الـ **OSI Model** فهي تقوم بتحديد خصائص وماهيات ووظائف المكونات المادية - الطبقة **1** في - **OSI** مثل شكل الكابلات، شدة التيار المتحكم بالإشارات الكهربائية الحاملة لرسائل المعطيات وما إلى ذلك بلإضافة إلى - خصائص الطبقة ٢ في - **OSI** مثل العنوان ماك **MAC Address** وبرتوكولات طبقة ربط المعطيات (**Data Link Layer**).

و لا تزال تقنيات الإيثرنت في تطور مستمر منذ نشوئها عام **١٩٧٩** بحيث تزداد قدرتها على التوسع الدائم واستيعاب أكبر عدد ممكن من الأجهزة المتصلة مع تأمين إمكانية النقل بسرعات عالية خلال أزمنة صغيرة وهذا ما يجعلها من أوسع تقنيات الشبكات المحلية انتشاراً وأكثرها استخداماً. و لشبكات الإيثرنت عدة أنواع من حيث السرعات المتوفرة وهي : Ethernet : تبلغ سرعة النقل فيها **Mbps Fast Ethernet : 10** تبلغ سرعة النقل فيها **Mbps Giga Ethernet : 100** تبلغ سرعة النقل فيها **Gbps 10 Giga Ethernet 1** تبلغ سرعة النقل فيها **Gbps 10** .

- **السرعات بشكل مختصر في شبكة الـ الايثرنت Ethernet :**

Ethernet = 10 MB | Fast Ethernet = 100 MB

Giga Ethernet = 1 GB | Ten Giga Ethernet = 10 GB

الوسط الفيزيائي (Medium) :

تستخدم شبكات الإيثرنت عدة أنواع من كابلات التوصيل وتختلف هذه الكابلات من حيث البنية والسعة العظمى للنقل (**Data Rate**) وهي:

الكابل المحوري : (**Coaxial Cable**) في المراحل الأولى للإيثرنت جرى استخدام كابل عرف باسم **ThickNet** قطره **10** ملم يتميز بمعدل نقل **10 Mbps** ويستخدم الآلية **BaseBand** لكشف الأخطاء، ويتيح طولاً أعظمياً للشبكة (**Network Span**) يقارب الـ **2500** متر، وعدد من العقد في المقطع يبلغ أعظمياً الـ **100** عقدة وبحيث لا يتجاوز طول المقطع الـ **500** متر ويعرف أيضاً باسم **10 Base5** حيث ترجع العشرة إلى معدل النقل والـ **Base** إلى آلية كشف الخطأ والـ ٥ إلى الطول الأعظمي للمقطع.

أما النوع الآخر من الكابلات المحورية فهو ما عرف باسم **ThinNet** قطره **5** ملم يتميز بمعدل نقل **10 Mbps** ويستخدم الآلية **BaseBand** لكشف الأخطاء، ويتيح طولاً أعظمياً للشبكة (**Network Span**) يقارب الـ **925** متر، وعدد من العقد في المقطع يبلغ أعظمياً الـ **30** عقدة وبحيث لا يتجاوز طول المقطع الـ **500** متر ويعرف أيضاً باسم **10 Base2** حيث ترجع العشرة إلى معدل النقل والـ **Base** إلى آلية كشف الخطأ والـ **2** إلى الطول

الأعظمي للمقطع، ونلاحظ أن هذا النوع من الكابلات عموماً أصبح نادر الوجود في الوقت الحالي.

و هناك نوع ثالث من الكابلات المحورية المستخدمة في شبكات إيثرنت تعرف بـ **10 Broad36** حيث يبلغ قطر الكابل ٠.٤-١.٠ سم يتميز بمعدل نقل **10 Mbps** ويستخدم الآلية **BroadBand** لكشف الأخطاء، ويتيح طولاً أعظمياً للشبكة (**Network Span**) يقارب الـ **3600** متر ولا يتجاوز طول المقطع الـ **1800** متر.

الكابلات المجدولة : **Twisted Pair** ولها نوعان هما **Shielded Twisted Pair** (**STP**) و (**UTP**) **Unshielded Twisted Pair** يختلفان اختلافاً بسيطاً في البنية بحيث أن الأول يعد أكثر مقاومة للتشويش ولكنه أعلى كلفة.

تستخدم شبكلا الإيثرنت النوع **UTP** حيث يبلغ قطر الكابل ٠.٤-٠.٦ سم يتميز بمعدل نقل **10 Mbps** ويستخدم الآلية **BaseBand** لكشف الأخطاء، ويتيح طولاً أعظمياً للشبكة (**Network Span**) يقارب الـ **500** متر ولا يتجاوز طول المقطع الـ **100** متر ويعرف أيضاً باسم **10 BaseT** .

و هناك سعات لكابلات الـ **UTP** تبلغ الـ **100 Mbps** يمكنها تخديم الـ **100 Mbps** إيثرنت وحتى الـ **Gigabit** إيثرنت وتوفير مسافات أعظمية أكبر للشبكة.

الألياف الضوئية : (**Optical Fiber**) أكثر كلفة من الـ **UTP** لاستخدامها تقنيات نقل أعلى وتستخدم غالباً في توصيل المبدلات (**switches**) والمركّزات **hubs** وليست شائعة الاستخدام في توصيا الحواسب والطرفيات إلى الشبكة نظراً لكلفتها المرتفعة.

التوصيف المعياري للـ IEEE للإيثرنت :

802.3x = Full Duplex

802.3ae = 10 GB

802.3at = POE

802.3u = 100 MB

8023ab = 1 GB



Ethernet Frame Format

صيغة إطار الايثرنت

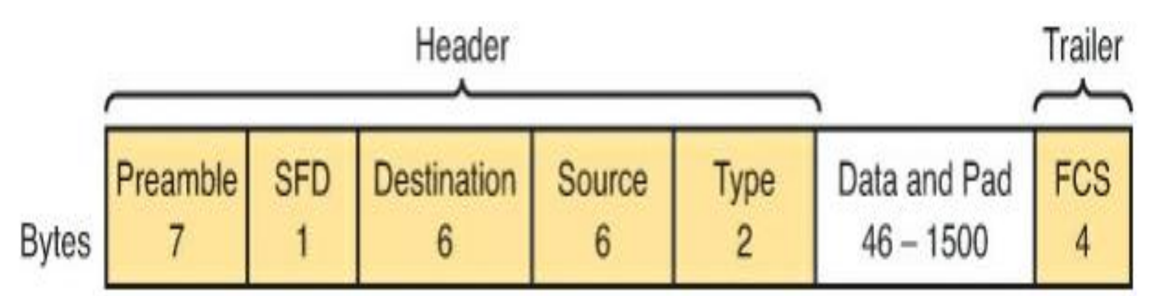
- **Ethernet Frame Format:** هي عملية تغليف البيانات و هي تعني إضافة معلومات على البيانات لكي يتم مساعدة هذه البيانات للوصول للطبقة الآخر ى، و حجم التغليف سيكون **26** بايت وسيتم تقسيمهم على **6** خانات .

Ethernet					
8	6	6	2	46 to 1500	4
Preamble	Destination Address	Source Address	Type	Data	Frame Check Sequence

- يتكون إطار الايثرنت من **Header** طول هذا الـ **Header 26 bytes** و يحتوي على **6** خانات يتم تركيبهما بشكل منظم وكل خانة تحتوي على معلومات و كل خانة له وظيفة خاصة .
- الأن سأقوم بذكر محتويات الـ **Ethernet Frame Header** التي يتكون منها الـ **Header** .

  1- **Preamble and Start Frame Delimiter Fields**
  2- **Destination MAC Address Field**
  3- **Source MAC Address Field**
  4- **Length/Type Field**
  5- **Data and Pad Fields**
  6- **Trailer Field / Frame Check Sequence Field**

- قبل إن نبداء في شرح التفاصيل يجب إن نعرف إن عملية التغليف تنقسم إلى قسمين كما في النموذج التالي :



- لاحظ في النموذج إنه منقسم لقسمين **Header** و **Tralier** و يوجد حقل مشترك ما بينهم **Data and Pad** في هذه الحالة يجب إن نكون على معرفة كيفية تكوين الـ **Header** يبداء من اليسار إلى اليمين بشكل منظم و مرتب , و يبداء في تجميع البيانات و يقوم بتركيب البيانات في كل خانة من الخانات بشاكل المناسب .

- **Preamble and Start Frame Delimiter Fields :**

حقل المقدمة Preamble وهو عبارة عن **7 Bytes** مهمتها تحديد بداية الإطار وتحقيق التزامن بين المرسل **Source** والمستقبل **Destination** لعملية بناء الإطار بشكل صحيح بمعنى إنه يقوم بجلب جميع المعلومات ليتم بناء الإطار على المعلومات التي حصل عليه .

- **DS = Destination MAC Address Field**

حقل عنوان المستقبل Destination MAC Address و هو عبارة عن **6 Bytes** مهمتها تحديد عنوان الماك ادرس لجهاز المستقبل , و عنوان الماك ادرس مستخدم من قبل الطبقة الثانية **Data Link Layer 2** و في هذه الطبقة يتم تحديد عنوان المرسل و عنوان المستقبل عن طريق الماك ادرس **MAC – Address** الخاص في كل جهاز من الطرفين , وقد يكون المستقبل عقدة وحيدة(**Uni Cast**) أو عدة عقد(**Multi Cast**) أو كافة عقد الشبكة (**Broad Cast**) .

- **AS = Source MAC Address Field**

حقل عنوان المرسل Source MAC Address Field

وهو عبارة عن **6 Bytes** لتحديد الـ **MAC Address** للمرسل ليتم تميز الـ **Frame** من اية جهاز مرسل و إلى اية جهاز مستقبل ليتم وصول الـ **Frame** للجهاز المطلوب بشكل صحيح .

- **Length / Type Field :**

حقل تميز أنواع الخانات Length/Type Field

ويستخدم لترميز البروتوكول المستخدم في الطبقة الأعلى التي ستمرر المعطيات إليها ويستخدم الترميز السداسي عشر فمثلاً بفرض كانت قيمته السداسية عشر هي عبارة عن **0800** فهذا يعني أن بروتوكول الطبقة العليا المستخدم هو بروتوكول الإنترنت **IP protocol** ، بينما تدل القيمة السداسية عشر **8137** على أن بروتوكول الطبقة الأعلى هو **IPX Protocol** .

- **Data and Pat Field :**

حقل البيانات Data and Pad Fields

وهو متغير الطول ويعبر عن المعطيات الفعلية التي يجري إرسالها والتي تجري عليها عملية **Framing** والتي سيجري تمريرها من الطبقة الثالثة **Data Link Layer 3** إلى طبقة إعلى الطبقة الرابعة الـ **Network Layer 4** المسؤولة عن عناوين الشبكات الاي بي **IP** و توجيه الـ **Packets** في الشبكة .

- **Trailer Field / Frame Check Sequence Field**

وهو عبارة عن **4 Bytes** يختتم به الإطار ويستخدم للكشف عن الأخطاء حيث تخزن فيه قيمة تدعى **Frame Check Sequence FCS** والتي يجري حسابها وفقاً لخوارزمية لكشف الأخطاء (**Cyclic Redundancy Check CSC**) والتي لها أنواع مختلفة ويجري تطبيقها على الحقول بدءاً من **DA** وحتى نهاية الإطار وأثناء الحساب تؤخذ قيمة **FCS** أصفاراً، وعند الاستقبال يقوم المستقبل بتطبيق نفس خوارزمية كشف الأخطاء وإيجاد الناتج ومقارنته مع الحقل **FCS** للتأكد من خلو الطرد من أخطاء أثناء عملية النقل.

- يجب إن نعرف إن مجموعة الحقول **Destination Address DA** و **Source Address SA** و **Type** تؤلف ما يسمى بالترويسة. **Header** كما ذكرنا سابقاً في بداية الدرس .

بنية الإطار: Ethernet 802.3 :

نلاحظ أن الحقول جميعها مطابقة للحقول السابقة عدا أحد حقول الترويسة وهو الحقل **Length** وهو نفس الـ **2 Bytes** السابقتين ولكنها تلعب دورا في تحديد الحقل **MAC- client data** وهو حقل جزئي من حقل البيانات **data** .

آلية الإصغاء في المنافذ المتعدد وكشف التصادم

Carrier Sence Multiple Access with Collision Detection CSMA/CD

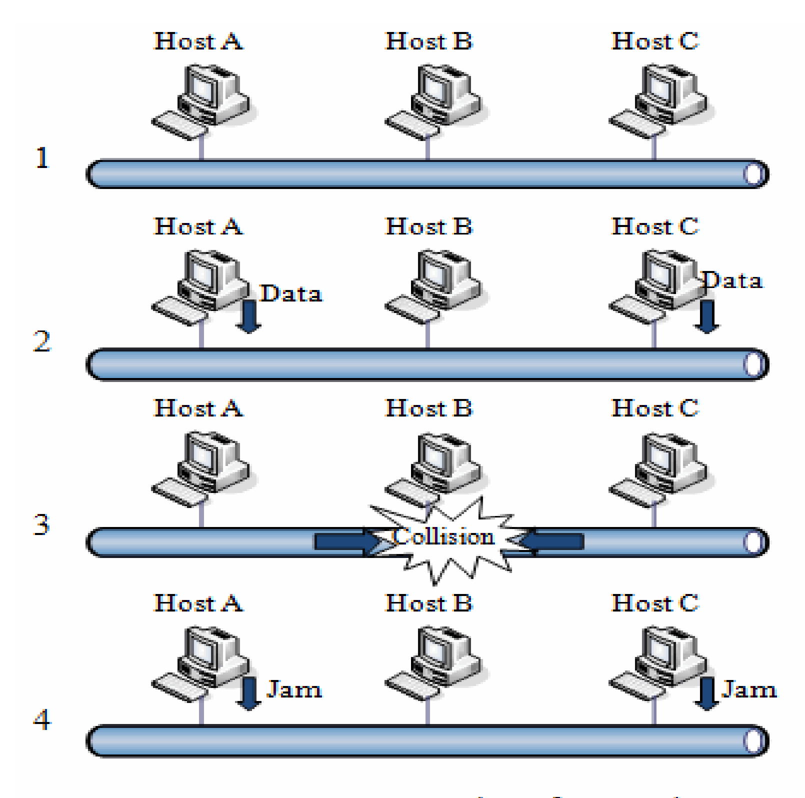


Figure 2.4. Principles of CSMA/CD

التصادم : تتصل العقد **A** و **B** و **C** و **D** جميعها إلى **Medium** وحيد فهي تؤلف مقطعاً **Segment**.. وبفرض أرادت العقدة **A** إرسال بيانيات للعقدة **B** عبر الشبكة، عندها سينتقل الطرد المرسل من **A** إلى كافة العقد المتصلة بالشبكة وستقوم كل منها بمقارنة عنوان الـ **MAC** الخاص بها مع عنوان المستقبل **D A** الوارد في الطرد لتتأكد إن كان الطرد يخصها وإلا فإنها تهمله (و هو ما تقوم به العقدتان **C** و **D** في هذه الحالة). و في حال كان عنوان المستقبل هو العنوان العام (**BroadCast**) ستعتبر كل عقدة من هذه العقد أن الطرد المرسل يخصها وستقوم بمعالجته. و بناء على هذه البنية يحدث التصادم في حال أرادت عقدتان إرسال إطار في وقت واحد.

الإصغاء : وتعني أن أي عقدة قبل أن تقوم بإرسال أي طرد إلى الوسط فإنها "تصغي" إلى الوسط أي تستشعر وجود إشارة حاملة **Carrier** يجري إرسالها على الكابل في الوقت الحالي.. وذلك بهدف معرفة إن كانت هناك عقدة أخرى في حالة إرسال أو كان الوسط فارغاً وجاهزاً لاستقبال طرد لإيصاله إلى باقي العقد. النفاذ المتعدد : ومعناه أن إي طرد يجري إرساله عبر الوسط يجري استقباله من كافة عقد الوسط (لأنها جميعاً في حالة إصغاء) ومن ثم اتخاذ القرار بإهماله أم معالجته.

كشف التصادم : يحدث التصادم عندما ا تستشعر عقدتان أن الوسط فارغ وتبدأان بإرسال الطرود في الوقت نفسه.. وبما أن أي عقدة متصلة بالشبكة تصغي إلى الشبكة في نفس الوقت الذي ترسل فيه طروداً عبر الشبكة لتتأكد من أنها العقدة الوحيدة المرسلة على الشبكة، فما يحدث عند التصادم هو أن العقدة المرسلة ستعود إليها الإشارة المرسلة ولكن بشكل مشوه (**grambled**) وعندها ستستشعر وجود التصادم وستتوقف عن الإرسال وتنتظر فترة زمنية حتى يتم تفريغ الوسط هذه الفترة الزمنية تدعى غرامة/زمن التأخير (**back off time/delay**) طول هذه الفترة عشوائي أي أنه يختلف من عقدة إلى أخرى وذلك لتفادي حدوث التصادم من جديد في حال قيام العقد بإعادة الإرسال بعد انقضاء نفس الزمن.

تقطيع الشبكة إلى عدة مقاطع: **Segmentation**

يؤلف المقطع الوحيد **Segment** مجال تصادم **Collision Domain** تصبح معالجة مشكلة التصادم عليه أعقد وأصعب وتستغرق وقتاً أكثر كلما زاد عدد العقد المتصلة بمقطع وحيد ومن هنا تظهر أهمية عملية تقسيم الشبكة إلى مقاطع متعدد تشكل مجالات تصادم متعددة **Multiple Collision Domain** يسهل حل التصادم على كل منها وفي نفس الوقت جرى توسيع للشبكة وإضافة عدد جديد من العناصر المنتمية للشبكة.

آليات مختلفة لتقطيع الشبكة: **Segmentation**

إن عملية التقطيع **Segmentation** قسمت الشبكة إلى عدة مقاطع غير متصلة مع بعضها.. فلا بد من إيجاد طريقة للوصل بحيث تستطيع عقد تنتمي إلى مقاطع مختلفة تبادل المعلومات فيما بينها، وهنا جرى استخدام نقاط (عناصر) وسيطة.. إذ لم تعد الشبكة في

هذه الحالة مؤلفة من عقد متصلة بكابل فحسب وإنما أصبحت الشبكة مؤلفة من نوعين أساسيين من الأجهزة:

النوع الأول يدعى عناصر الشبكة الطرفية (**Data Terminal Equipment DTE**) وتتمثل بكل ما الأجهزة التي بإنمإنها إرسال البيانات واستقبالها.

و النوع الثاني يدعى عناصر الشبكة الوسيطة (**Data communication equipment DCE**) نقاط وسطى تستقبل الطرود من جهة وتمررها إلى جهات أخرى وفق آليات مختلفة وتتمثل في أجهزة مثل مكرر الإشارة (**Repeater** نفس مبدأ عمل المركّز **Hub** تقريباً) والـ **Bridge** والمبدّلة **Switch** والـ **Routers** وجميعها تمثل صلة الوصل بين أكثر من مقطع **Segment** وتتيح توسيع حجم الشبكة كما تعتبر بطاقات الشبكة **Network Interface Cards NICs** من أحد أنواع عناصر التواصل في الشبكة.

استخدام المركّز **Hub** أو بين مقاطع الشبكة:

يقوم المركّز **Hub** ببساطة بتمرير الإطار **Frame** الوارد إلى دخله إلى كافة مخارجه أي أنه يمرر أي إطار متواجد على أي من المقاطع المتصلة به إلى كافة المقاطع الآخر حيث يجري تعميمها على كافة العناصر المرتبطة بهذا المقطع **Segment** ولكن هذه الطريقة في تعميم الإطارات تسبب الكثير من الهدر في عمليات النقل وهذا ما يجعل استخدام محصوراً بالشبكات الصغيرة التي تتميز بمعدلات منخفضة من المعطيات التي يجري نقلها.

استخدام الـ **Bridge** بين مقاطع الشبكة:

يصل الـ **Bridge** بين مقاطعن مختلفة من الشبكة ولكنه يختلف عن المركّز **Hub** بأنه يختبر عنوان المستقبل فلا يقوم بإرسال الإطار من المقطع الحاوي على العقدة المرسلة إلى كافة المقاطع المتصلة به وإنما يرسله فقط إلى المقطع الحاوي على العقدة ذات العنوان المستقبل.. أي أن الـ **Bridge** يصل بين مقطعين فقط على عكس المركّز **Hub** الذي كان يصل بين مقطع من جهة وعدة مقاطع من جهة أخرى.

و في حال كان المرسل والمستقبل ينتميان إلى نفس المقطع فإن الـ **Bridge** لا يقوم بتمرير إي إطار إلى أي مقطع خارجي آخر وهذا ما يجعله قادراً على القيام بعمليات نقل داخلية (ضمن مقطع واحد) متعددة في أكثر من مقطع في الوقت نفسه (على التوازي).

استخدام المبدّلة **Switch** بين مقاطع الشبكة:

تتألف المبدّلة **Switch** من عدة بوابات **Ports** تتصل كل منها بعنصر شبكة وحيد قد يكون - **DCE** مثل المركّز **Hub** أو الموزع **Switch** أخرى مثلاً- أو - **DTE**كأن يكون حاسباً أو طابعة أو. أي أن المبدّلة **Switch** تصل بين عدة مقاطع كل مقطع مؤلف من عقدة **Node** وحيدة متصلة بالكابل مما يجعل الشبكات التي تستخدم المبدّلة **Switch** (**Switched Networks**) خالية تماماً من التصادم. **Collision Free**

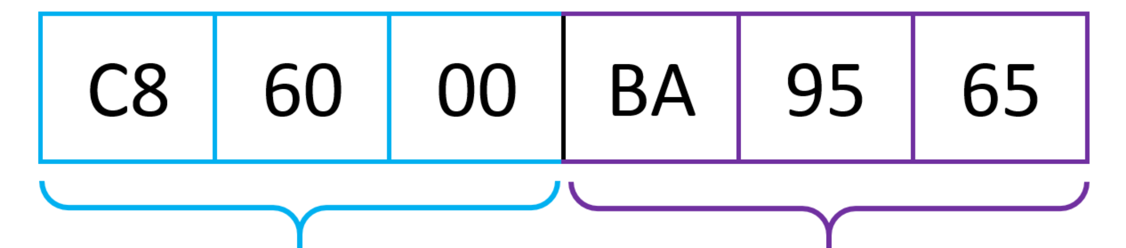
تقوم المبدّلة **Switch** باستقبال الطرد من المرسل وتحديد وجهة هذا الطرد.. وبما أن كل مقطع **Segment** متصل إلى أحد بوابات المبدّلة **Switch** مؤلف من عنصر وحيد فإن عنوان المستقبل سيجري تمريره إلى منفذ **port** وحيدة متصلة مباشرة بالمستقبل نفسه وبالتالي تمرير الإطار إلى الجهة المستقبلة لوحدها دون شغل أي عنصر من عناصر الشبكة باستقبال إطار قد لا يخصه.

تعمل المبدّلة **Switch** بإحدى التقنيتين **Full Duplex technology** : أو **Half Duplex Technology**

حيث تعني التقنية **Half Duplex** أن كل منفذ **port** من منافذ المبدّلة **switch** وما يتصل به من **DCE** أو **DTE** أو **NIC** يستطيع أن يقوم بالإرسال فقط أو الاستقبال فقط في وقت واحد.

أما التقنية **Full Duplex** تعني أن المنفذ **port** وما يتصل به يستطيع أن يقوم بإرسال البيانات واستقبالها في وقت واحد مما يضاعف من عرض الحزمة.. فمثلاً إن كان معدل النقل يعادل **100 Mbps** وكانت التقنية المستخدمة هي **Full Duplex** فهذا يعني أن سرعة النقل المجملة أصبحت تعادل **200 Mbps** .

Media Access Control OR Mac Address



يعتبر العنوان ماك ادرس أو (**Media Access Control**)قيمة فريدة تُربط ببطاقة الشبكة من قبل المصنع للتمييز ما بين بطاقات الشبكة الموجودة على شبكة محلية .(**LAN**) والمفروض أن يكون هذا العنوان مميز عالمياً أي لا توجد أي بطاقة شبكة أخرى في العالم تأخذ نفس عنوان الماك .

و بما أنه يُحدد من قبل الشركة الصانعة فغالباً ما يتضمن رقم الشهادة المسجلة الخاص بهذه الشركة. و بما أنه يعمل في الطبقة (**Data Link**) حسب التصنيف **OSI** والتي يمكن اعتبارها طبقة فيزيائية فقد تسمى بأسماء أخرى أحياناً مثل **Ethernet Hardware :** **Address (EHA)** ، **hardware address** ، **physical** , **adapter address** **address.**

في الشبكات التي تستخدم البروتوكول **TCP/IP** يمكن الاستعلام عن العنوان ماك لبطاقة شبكة بالإضافة إلى الـ **IP** عن طريق البروتوكول (**ARP**) أي **Address Resolution Protocol** من أجل الـ (**IPv4**) ، والبرتوكول(**NDP**) أي **Neighbor Discovery Protocol** من أجل الـ .(**IPv6**) على الشبكات التي تقوم بالإرسال بشكل **broadcast** -مثل شبكات الـ – **Ethernet** يقوم العنوان ماك بتعريف وتمييز كل عقدة على الشبكة ويسمح بتأشير كل (**Frame** مجموعة البتات المرسلة) لمعرفة الجهاز الذي يجب أن يستقبلها.و لذلك فإن العنوان ماك يشكل معظم الأساسيات التي تستند إليها طبقة الـ **Data link** من التمثيل **OSI** والتي تستند عليها بروتوكولات الطبقات الأعلى لتشكيل شبكات معقدة وفعالة.

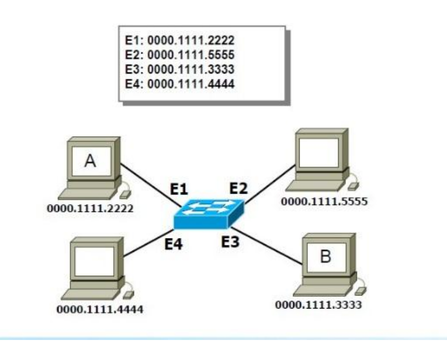
التقليد العالمي المتبع لكتابة العنوان ماك :

إن المعيار **IEEE 802** هو التنسيق المتبع لطباعة عناوين الماك من النمط **MAC-48** بشكل سهل ومألوف. حيث يتألف فيه العنوان من ست مجموعات تتألف كل منها من رقمين بالنظام السداسي عشر ويتم الفصل بين كل مجموعتين بخط صغير **(-) أو** بنقطتين **(:)** وترتب هذه الأرقام بحسب الإرسال. مثال**address2 01:23:45:67:89:ab :** أو **address1 01:23:45:67:89:ab** ويوجد تقليد آخر متبع من قبل **Cisco** وهو باستخدام ثلاث مجموعات كلٍ منها مؤلف من أربع أرقام بالنظام السداسي عشر، يفصل بينها نقط. مثال: **0123,4567,89 ab** وذلك حسب ترتيب الإرسال.

جدول العناوين الفيزيائية

MAC Address Table

- **جدول العناوين الفيزيائية :** هو الجدول الذي يتم بنائه في داخل جهاز السويتش و يحتوي على العناوين الفيزيائية و رقم المنفذ للأجهزة المتصلة بجهاز السويتش مما يمكن السويتش بان يرسل البيانات إلى جهاز المرسل اليه مباشرة .
  جدول العناوين لديه اكثر من اسم يطلق عليه **Forward filter Table** و **Content Addressable Memory** و **Physical Address** و **MAC Address Table**

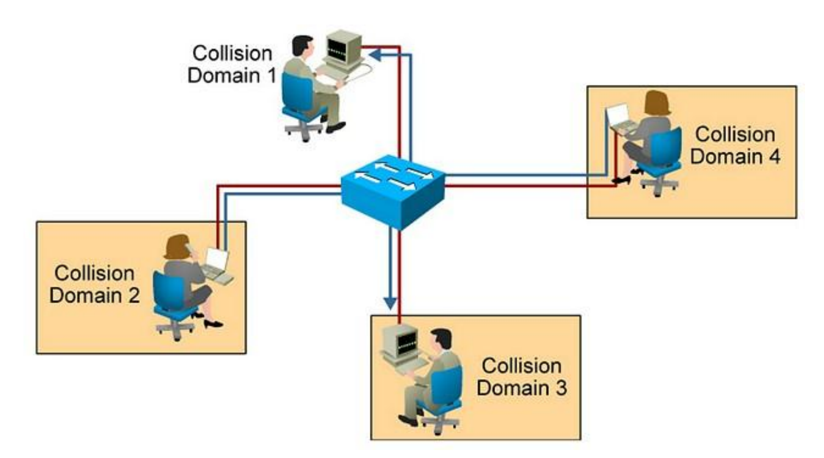


المبدل Switch



المبدل Switch : هو عبارة عن جهاز متعدد المنافذ مثل الـ **Hub** ولكن جهاز المبدل أو السويتش عندما ا نقوم بتشغيله يقوم بعملية فحص الفريمات التي تأتية من كل جهاز متصل في منافذ المبدل حيث يقوم بأخذ الـ **Source MAC Address** و يقوم بتسجيلها في جدول العناوين الفزيائية الموجود في داخل المبدل .

- **ملاحظة مهم جداً :** عندما يقوم بأخذ الـ **Source MAC Address** لكل جهاز سيقوم بتسجيل العنوان و مقابله رقم المنفذ المتصل فيه ليتم التعرف عليهم و تسجيلهم في الجدول .
- كل منفذ من منافذ المبدل أو السويتش هي عبارة عن مجال تصادم واحد بمعنى إنه مجال التصادم موجود على كل منفذ من المنافذ وليسه على كل السويتش **One Collision Domain ,** و هذا النظام افضل بكثير من إن يكون جميع المنافذ في مجال تصادم واحد مما يجعل كل منفذ يعمل بسرعة خاصة فيه مثل لو وجد منفذ بسرعة **100 Mb** هذه السرعة ستكون خاصة في المنفذ ولا يستطيع منفذ اخرى مشاركة هذه السرعة و كل منفذ يكون له سرعة مستقلة خاصة فيه و غير مشتركة .



Switch Three function

وظائف المبدل أو السويتش

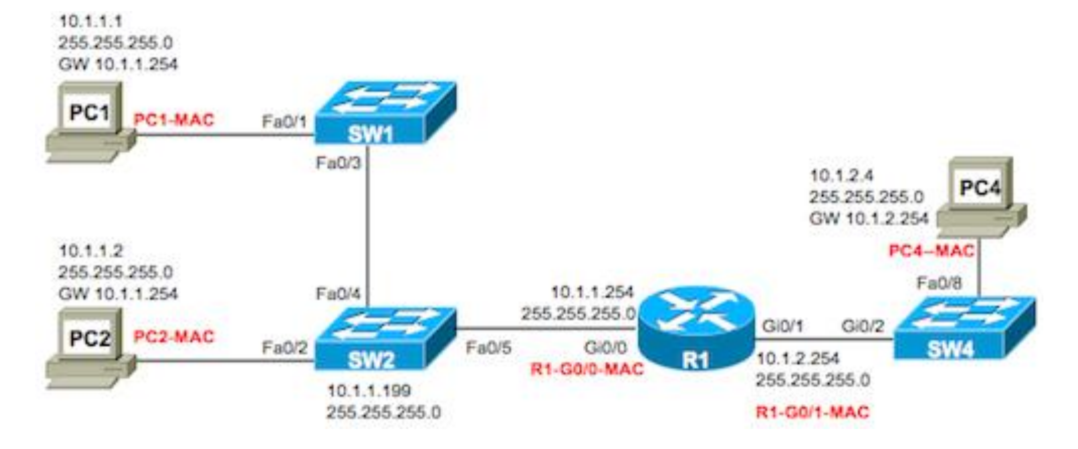


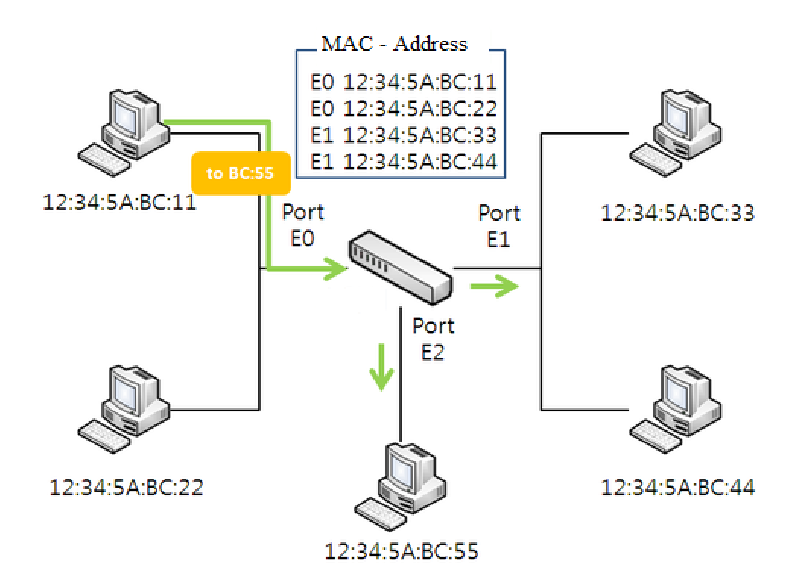
- يقوم المبدل بثلاثة وظائف اساسية و من المهم جداً أن نتعرف عليهم و نعرف كل واحد ما هي وظيفة كل واحدة سأقوم بذكرهم و شرحهم .

1- Address Learning تعلم العناوين
2- Filtering / Forwarding Deision عملية التصفية و الإرسال
3- Loop Avoidance منع دوران البيانات

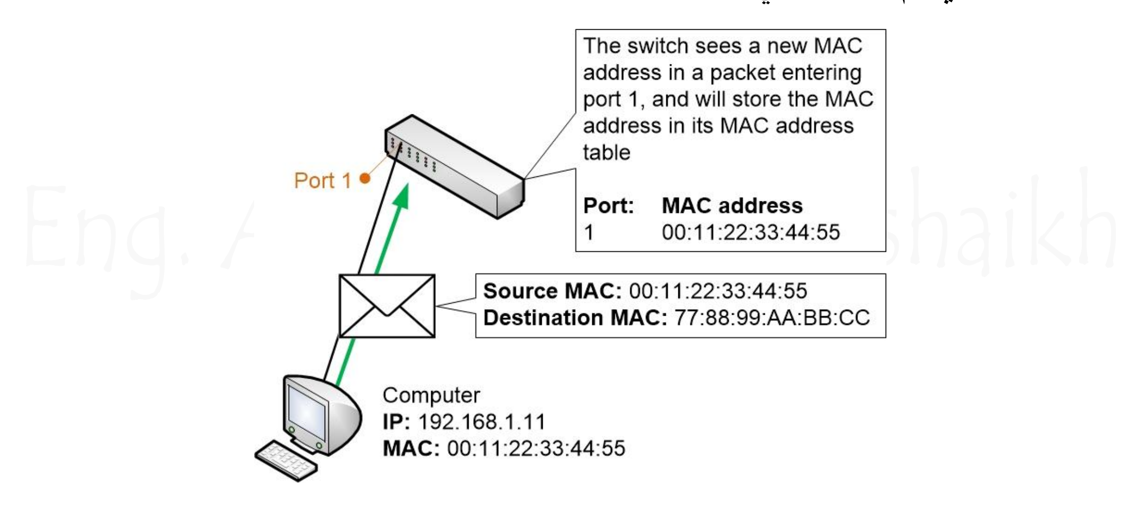
- هذه هي الوظائف الثلاثة التي تعمل في داخل السويتش أو المبدل سأقوم بشرح كل واحد بشكل منفصل عن الآخر لنفهم وظيفة كل منهم و ماذا تفعل و متى ياتي دور هذه الوظيفة في داخل المبدل .

- **Address learning تعلم العناوين:** هذه الوظيفة هي المسؤولة عن معرفة العناوين الفيزيائية **MAC - Address** للأجهزة المتصل في المبدل حيث تقوم بمعرفة العناوين عن طريق عمل البث المباشرة **Broad Cast: ffff.ffff.ffff** بهذه العملية يستطيع المبدل معرفة جميع العناوين الفيزيائية و تسجيله في جدول العناوين الموجود في داخل المبدل و حيث يقوم بتخزين العنوان و رقم المنفذ المساوي اليه كما في النموذج التالي....



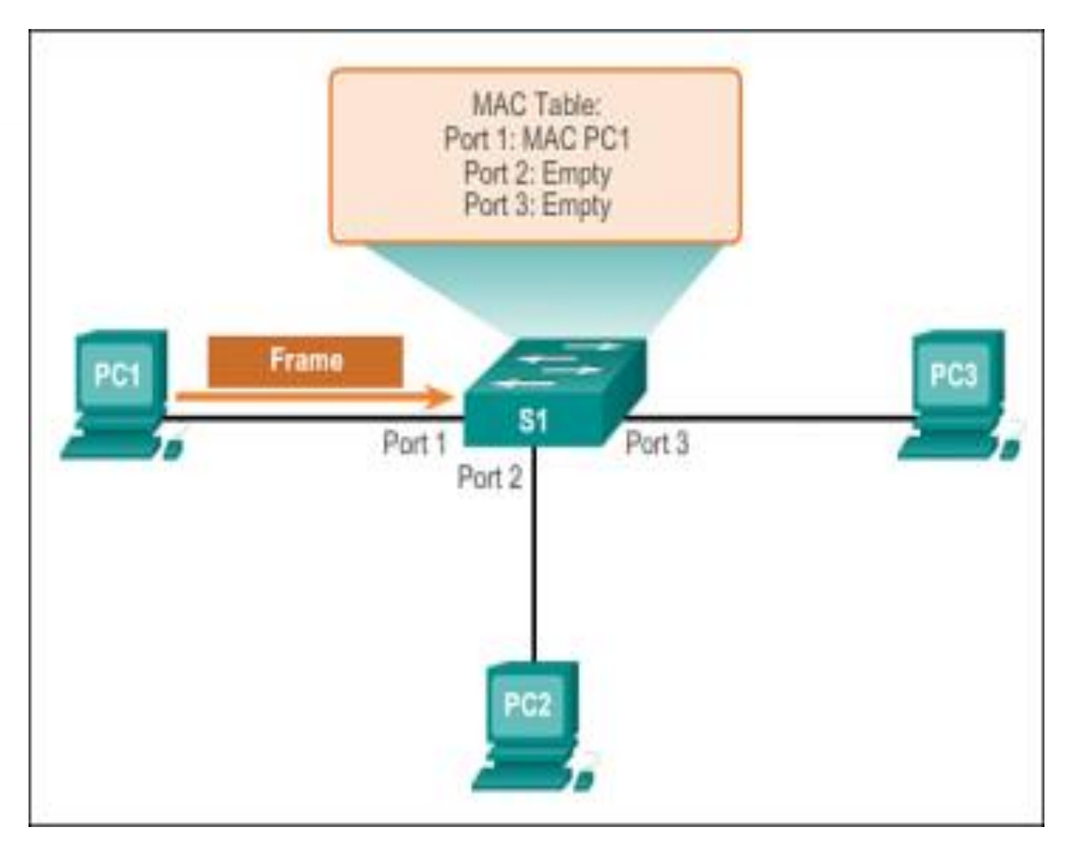


- لاحظ إن كل عنوان ماك ادرس متساوي مع المنفذ المتصل فيه الجهاز صاحب الماك ادرس الذي تم تسجيله في جدول العناوين الفزيائية .

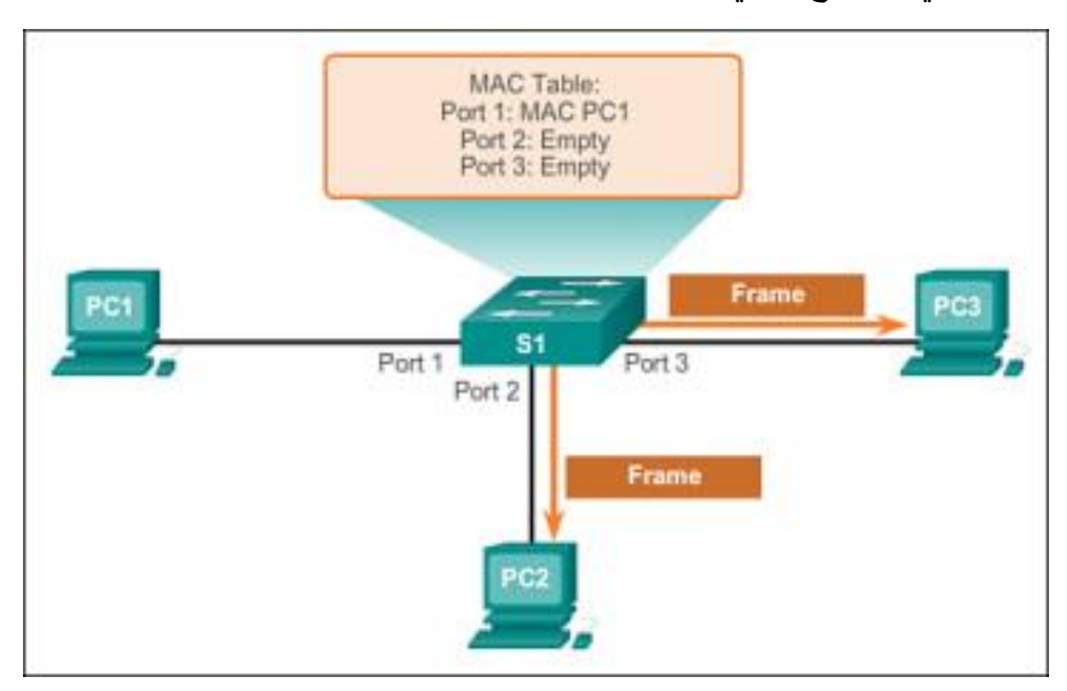


Filtering / Forwarding Deision عملية التصفية و الإرسال: هذه الوظيفة تبداء في العمل عندما يرد جهاز متصل في المبدل أو السويتش يريد أن يرسل **Frame** لجهاز اخر متصل معه على المبدل من الطبيعي جداً إن الجهاز الذي يريد إرسال رسالة للجهاز المطلوب يجب إن يكون على معرفة بعنوان الماك ادرس الخاص في الجهاز المرد الإرسال اليه الأن سنقوم بشرح مثال على النموذج التالي لنفهم كيفية الإرسال بشكل مباشر و من دون إن بإرسال الرسالة لجميع الأجهزة المتصلة معه في الشبكة تابع النموذج التالي.....

في هذا النموذج سيتم إرسال رسالة الـ **Frame** من جهاز الـ **PC1** إلى **PC2** و **PC3** سيتم إرسال الـ **Frame** الـ **Switch** المبدل سيقوم بنظر في الرسالة و يحدد العناوين التي سيتم الإرسال اليه و يقوم بإرسال الـ **Frame** للجهاز المطلوب بشكل اتوماتيكي مع العلم لان يتم إرسال الرسالة لجهاز اخر لأنه في داخل الرسالة تم تحديد العناوين الفزيائي.

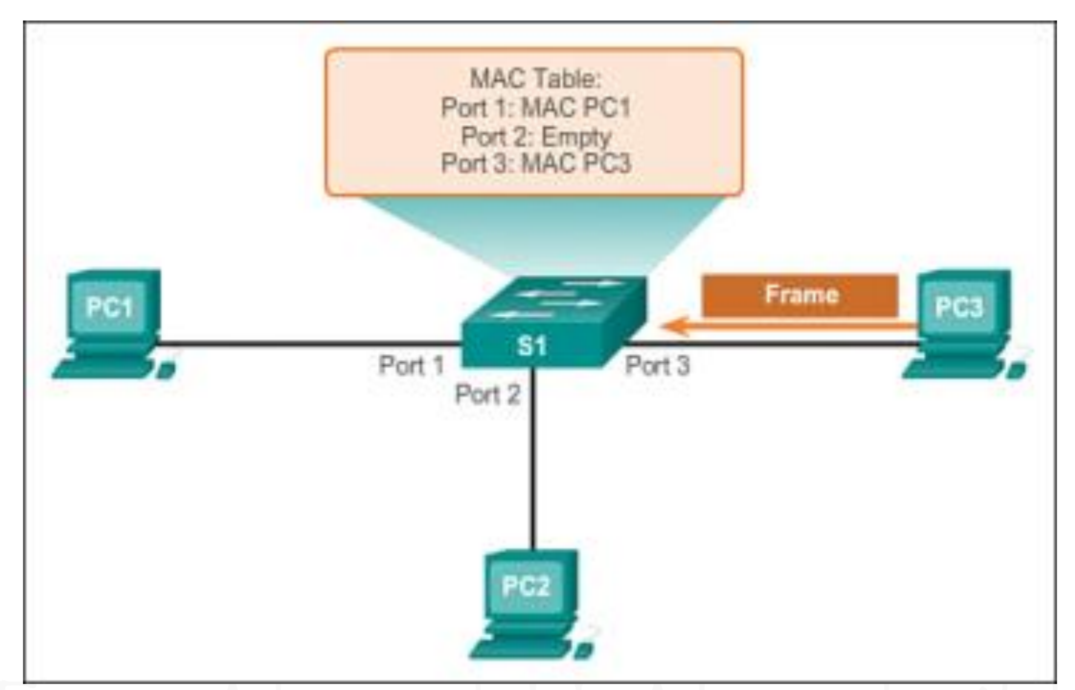


- لاحظ في النموذج تم إرسال الـ **Frame** للمبدل في هذه الحالة يقوم بنظر في داخل الـ **Frame** ليعرف اي العناوين التي يجب أن ترسل اليه الرسالة و في هذه الحالة تم التعرف على **PC2** و **PC3** سيقوم بإرسال الرسالة بشكل مباشر لهذه الأجهزة فقط مثل ما في النموذج التالي ....

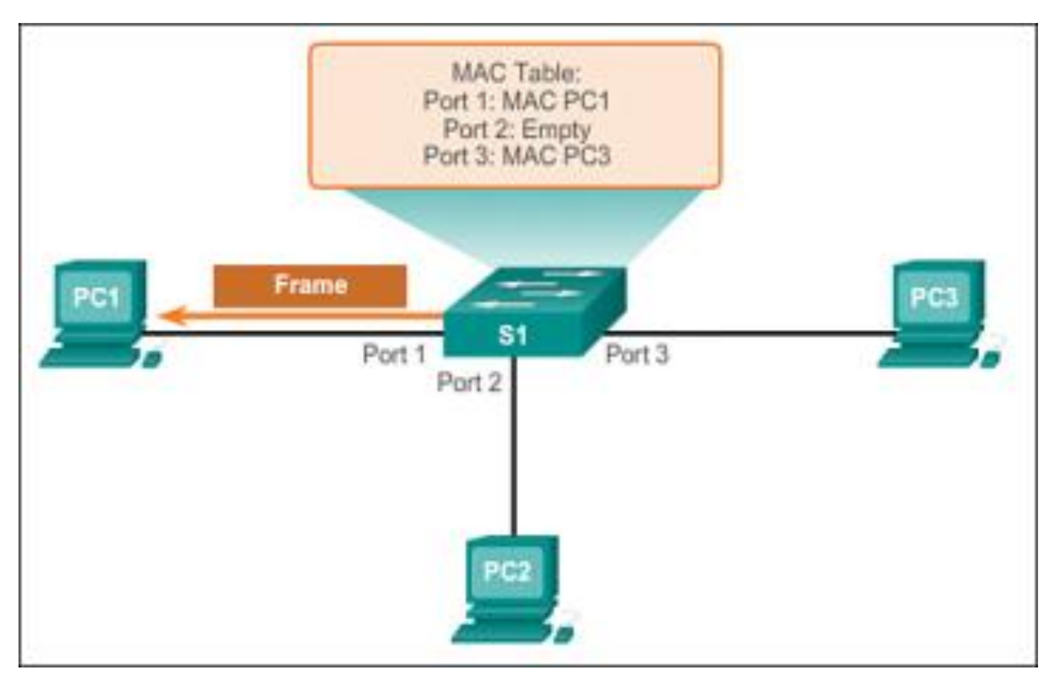


- الأن كما نرى في النموذج إنه تم وصول الـ **Frame** للأجهزة المطلوبة بشكل صحيح الأن سنرى نموذج ثاني لنفهم اكثر هذه العملية بشكل اقرب ....

- في هذا النموذج يرد جهاز **PC3** إرسال رسالة لجهاز **PC1** سيقوم الجهاز بإرسال الـ **Frame** للمبدل سيقوم المبدل بقراءة هذه الـ **Frame** ليعرف إلى إين متجه هذه الرسالة و بعد أن يعرف سيقوم بتحديد الجهاز عن طريق العنوان الفزيائي و تحديد المنفذ المتصل عليه ليتم الإرسال بشكل مباشر اليه كما في النموذج التالي ....

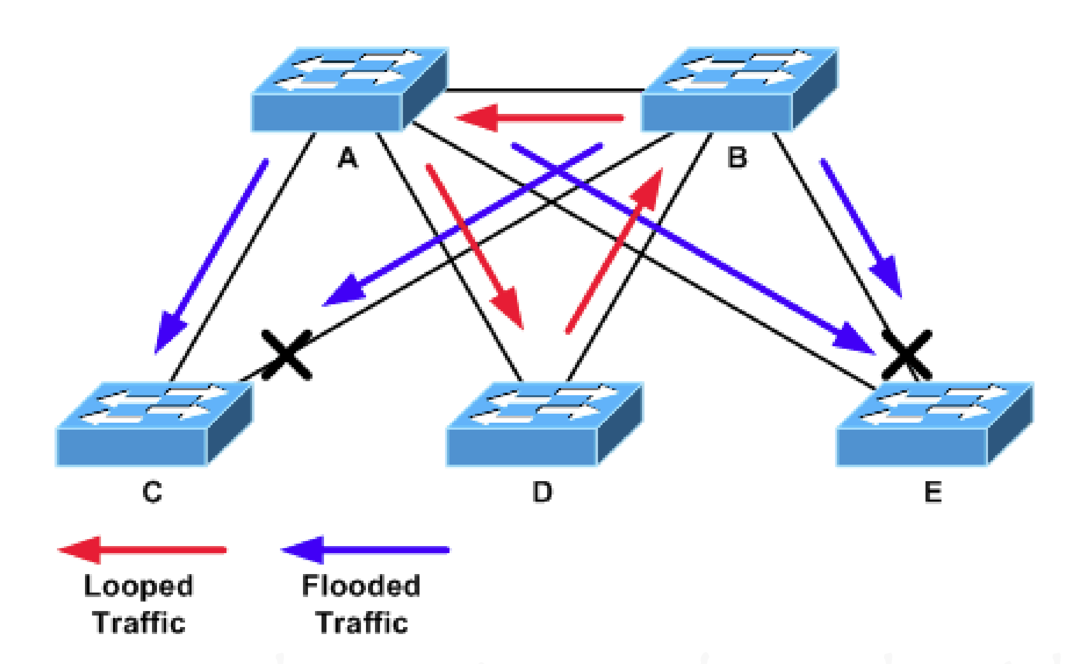


- أنظر تم وصول الـ **Frame** للمبدل و قام بقراءة الـ **Frame** و في هذه الحالة تم التعرف على الجهاز المطلوب سيقوم الأن بإرسال الرسالة اليه و هو الجهاز **PC1** المتصل على المنفذ **Port 1** كما في النموذج التالي ....

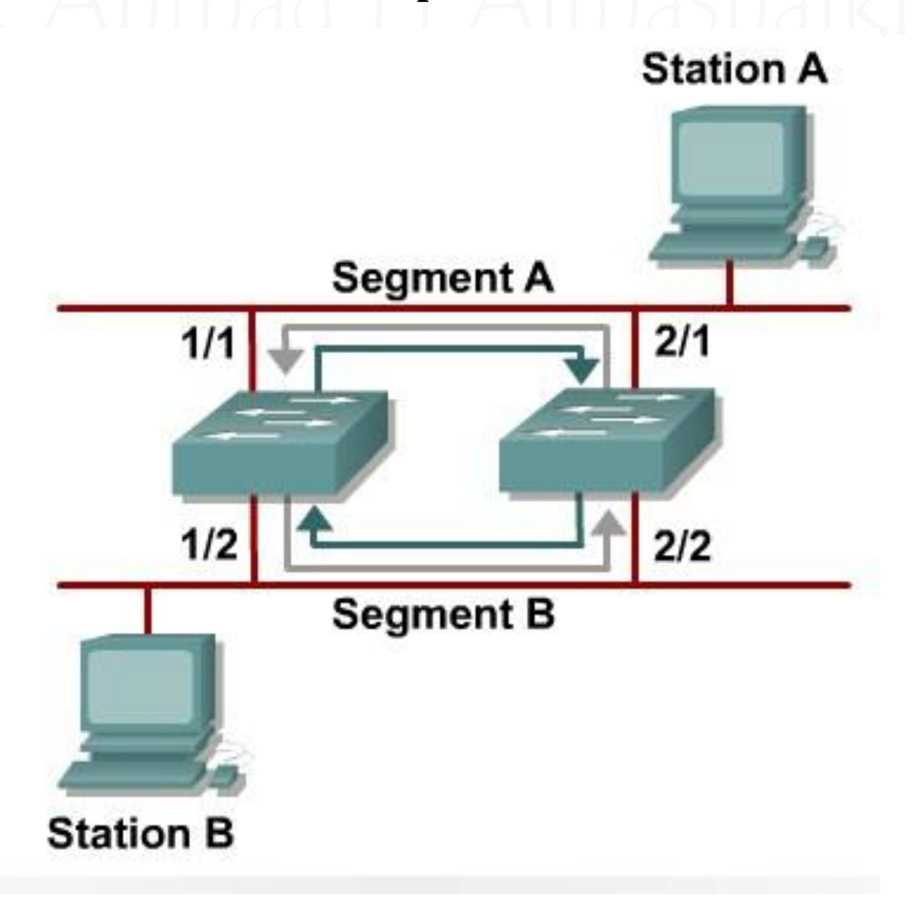


- لاحظ الأن تم وصول الـ **Frame** إلى الجهاز **PC1** بهذا الشكل تكون قد تم وصول الرسال للجهاز المطلوب بشكل صحيح .

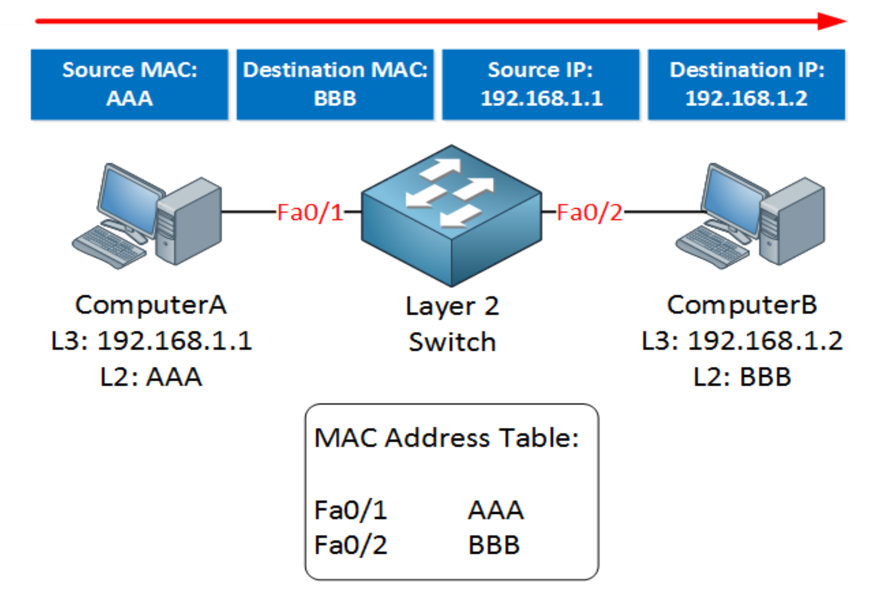
Loop Avoidance منع دوران البيانات: هذه الوظيفة المسؤولة عن منع دوران البيانات في داخل المبدل (**Switch**) في حال تم ربط اكثر من سوتيش سيحصل عملية دوران البيانات ولكن في داخل السويتش يوجد بروتوكول يمنع دوران البيانات في داخل السويتش و هذا البروتوكول الـ **STP** سنتعرف عليه بشكل كبير جداً في الدروس القادمة.



Loop



طريقة إرسال الـ Frame في داخل المبدل (Switch)



يوجد ثلاث طرق تعتمد الـ Frame على عليهم في عملية الإرسال سأقوم بذكرهم و شرح كل واحد منهم :

1- Store and Forwarding هذه الطريقة المعتمد في أجهزة سيسكو لعملية الإرسال
2- Cut – Through هذه طريقة إرسال البيانات للجهاز المطلوب من دون تخزينه
3- Fragment – Free هذه العملية المسؤولة على تاكيد إرسال البيانات بشكل صحيح

- **Store and Forwarding تحتوى على قسمين سأقوم بذكرهم :**

١- **Error Checking:** التاكد من عدم وجود اخطاء بعد استلام الـ **Frame** القادمة للدخول في عملية التكوين من جديد **Header**.

٢- **Automatic Buffering :** التخزين المؤقت الأتوماتيكي تقوم هذه العملية بمعالجة البيانات و تحديد السرعة المستخدمة و المنفذ الذي سيقوم بعملية الإرسال و بعده يقوم بإرسال الـ **Header** إلى **FCS check** للتاكد من عدم وجود اخطاء في الـ **Frame** لتتم عملية الإرسال , كل هذه العملية تكون بشكل مؤقت في عملية التكوين في داخل الـ **Buffering**.

٣- **Cut – Through تحتوى على قسمين سأقوم بذكرهم :**

١- **Rapid Frame Forwarding:** هذه العملية المسؤلة عن إرسال البيانات بشكل سريع من دون تخزينها مثل عندما جهاز ما يريد إرسال رسالة لجهاز آخر سيقوم الجهاز بإرسال الرسالة بشكل مباشر للجهاز المطلوب من دون تخزين الرسالة.

٢- **Fragment Free :** هذه العملية تقوم بتحرير الاجزء الخاص في الـ **Header** على اشكال قطع لتصل جميع البيانات إلى حقل البيانات ليتم التاكد من هل حدث خطاء أو هل يوجد بيانات تم تجاوزه هذه وظيفة الـ **Fragment**.

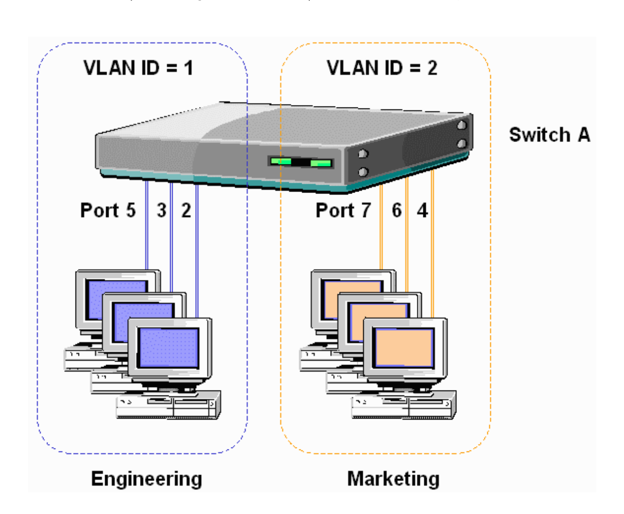
Cisco Switch Configuration

Command

Switch > **?**	All Command
show mac address-table address	Displays MAC address table information for the specified MAC address
show mac address-table aging-time	Displays the aging time in all VLANs or the specified VLAN.
show mac address-table count	Displays the number of addresses present in all VLANs or the specified VLAN.
show mac address-table dynamic	Displays only dynamic MAC address table entries.
show mac address-table interface	Displays the MAC address table information for the specified interface.
show mac address-table learning	Displays MAC address learning status of all VLANs or the specified VLAN.
show mac address-table static	Displays only static MAC address table entries.
show mac address-table vlan	Displays the MAC address table information for the specified VLAN.
end	Return to privileged EXEC mode.
show mac address-table learning [vlan vlan-id | interface interface slot/port]	Verify the configuration.
copy running-config startup-config	(Optional) Save your entries in the configuration file.

Virtual Local Area Network (VLAN)

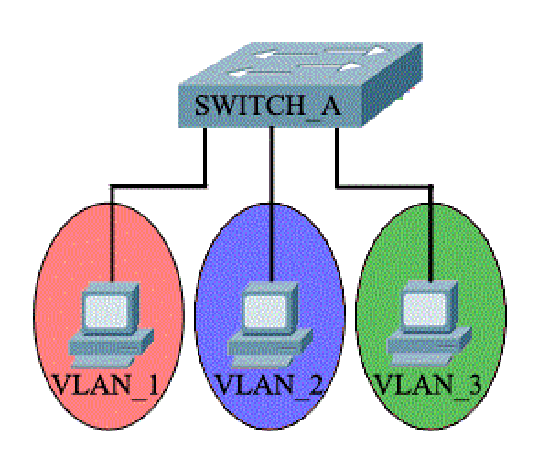
الشبكة المحلية الافتراضية



Vlan : هي عبارة عن شبكة وهمية موجودة في داخل سويتشات سيسكو فقط و يتم العمل على هذه الشبكة الوهمية عن طريق تقسيم منافذ السويتش إلى عدة شبكات كل منها منفصله عن الآخر بشكل وهمي وغير مرئي ولا يمكن لي أجهزة الحاسوب التي في شبكة معينة من شبكة الـ**Vlan** أن تتصل في أجهزة حاسوب اخرى في شبكة **Vlan** مع العلم إنهم على سوتيش واحد و تحت نتطاق واحد ولكن عندما يتم تقسيم الشبكات ستكون كل شبكة في نطاق وهمي مختلف عن النطاق الآخر في داخل السوتيش.

مثال على تقسيم شبكة الـ **Vlan** في داخل السويتش :

- **أنظر للنموذج التالي يوجد فيه ثلاث شبكات Vlan 1, Vlan 2, Vlan 3 و كل شبكة تاخذ عنوان اي بي مختلف عن الآخر .**



Vlan 1 ip: 192.168.1.1

Vlan 2 ip: 192.168.2.1

Vlan 3 ip: 192.168.3.1

في هذه الحالة شبكة **Vlan 1** الأجهزة المرتبطة فيها لا تستطيع الاتصال بشبكة **Vlan 2** و لا شبكة **Vlan 3** لأنه تم تقسيم السويتش لثلاث شبكات مختلفة عن بعضهم العبض ولو اردنا الشبكة أن تتصل مع بعضها البعض نحتاج لجهاز الموجه أو الراوتر لجعل الشبكات تتصل مع بعضها البعض هذا كان مثال لشبكة الـ **Vlan** .

ملاحظة : السويتشات التي تدعم شبكة الـ **Vlan** فقط سوتيشات سيسكو .

- **الفرق بين الـ Vlan و Subnetting :**

١- الـ **Subnetting** هو مفهوم تقسيم عنوان الشبكة **IP Address** الواحد إلى عدة عنوان شبكة **IP Address** فرعية بغض النظر عن فئة العناوين **A,B,C** مع العلم إنه هذا المفهوم غير خاص في جهاز معين مثل الراوتر أو السويتش .

٢- **Vlan** تستخدم لتقسيم السويتش لعددة اجزاء بمعنى تقسيم المنافذ لعددة شبكات و فصل الشبكات عن بعضها البعض.

- **مميزات و فوائد شبكة الـ Vlan :**

١- التقليل من عملية البث المباشر **BroadCast** .

٢- سهولة في ادارة و صيانة الشبكة .

٣- يسهل إضافة جهاز في اي شبكة .

٤- سهولة نقل جهاز من شبكة لشبكة اخرى من دون الحاجة لنقل اسلك من منفذ لمنفذ.

٥- افضل من ناحية الحماية و الامن , مثل لو تم تسريب فيروس أو تم اختراق شبكة معين لا ستطيع الفيروس أو المخترق الوصول للشبكة الآخر هذه نقطة في حق شبكة الـ **Vlan**.

٦- **Vlan** هي جزء من الـ **BroadCast Domain** ويتم تقسمه إلى اجزاء و تعتبر الـ **BroadCast Domain** مستقلة بذاتها و هذه من صالح الشبكة حيث يتم تقليل مجال تصادم البيانات و الاختناق و الضغط في المسارات.

أنواع الـ Vlan

Type of Vlan

- يوجد عدة أنواع من شبكة الـ **Vlan** و كل نوع لديه وظيفة معين سأقوم بذكرهم و شرحهم .

1- Data Vlan
2- Default Vlan
3- Native Vlan
4- Voice Vlan
5- Management Vlan

Data Vlan : هذا النوع من شبكة الـ **Vlan** تستخدم في إرسال البيانات للمستخدمين على الشبكة، و عادة تستخدم هذه الشبكة في الشبكة الصغيرة و تقوم بعمل جميع الوظئف مثل شبكة الصوت و الشبكة الآخر ، اما في الشبكة الكبيرة تكون هذه الشبكة فقط لنقل المعلومات ما بين الشبكات.

Default Vlan : هذا النوع من شبكة الـ **Vlan** تكون موجود في داخل السويتش بشكل تلقائي و تاخذ الرقم واحد، و يكون جميع منافذ السويتش تحت هذه الشبكة في حال لم يكون هناك شبكة **Vlan** تم اضافته من الطبيعي جداً أن تكون جميع المنافذ تحت هذه الـ **Default Vlan** و يتم الاعتماد عليه في كثير من الاعمل و تستخدم بروتوكولات مثل **STP, CDP, VTP,** ، مع العلم هذه الشبكة لا يمكن حذفها أو اعادة تسميتها لي إنها تحتوي على بروتوكولات ولذلك لا يمكن التعديل عليه و سنعرف أن هذه الشبكة هي اساسية في جهاز السويتش .

Native Vlan : هذه الشبكة تساوي شبكة الـ **Default Vlan** و تعتبر نفس الشبكة ولكن الـ **Native Vlan** تعتمد على بروتوكول الـ **IEEE 802.1Q** ويتم من خلاله تنقل الترافيك بوضع علامة الـ **Tag** وحجم الترافيك أو التغليف سيكون **4 byte** سأقوم بشرح هذا البروتوكول في الدروس القادمة.

Voice Vlan : هذه الشبكة مخصصة في شبكة الصوت **Network Voice** و وظيفة شبكة الـ **Voice Vlan** عزل شبكة الداتا عن شبكة الـ **Voice** لأن شبكة الصوت تعتبر شبكة مهم جداً ولا يمكن للرسال الصوتية أن تنتظر مثل الداتا لهذا السبب يوجد شبكة الـ **Voice Vlan** مخصص فقط لشبكة الـ **Network Voice** .

Management Vlan : هذه الشبكة مختصة في ادارة السويتش و التي تستخدم في عملية المراقبة و الاتصال في اكثر من سويتش و العمل مع بروتوكولات مثل **HTTP** **Telent , SSH , SNMP** و تستخدم ايضاً لي ادارة شبكات الـ **Vlan** .



أرقـــام الـ Vlan

Vlan ID Range

- أرقام شبكات الـ **Vlan** كل شبكة **Vlan** تاخذ رقم لا يتكرر لشبكة اخرى ليتم تميز الشبكة عن بعضها البعض , و يوجد رنج معين لعملية بداء استهلك هذه الارقام و مع تتطور عالم الشبكات تم استهلاك الارقام الأولى التي سنقوم بذكرها الأن , و قاوم بتوسيع هذه الارقام لتصبح اكبر من العدد الأول سأقوم بذكر هذه الارقام .

1- **Normal Range From 1 up to 1005**
2- **Extended Range From 1006 up to 4096**

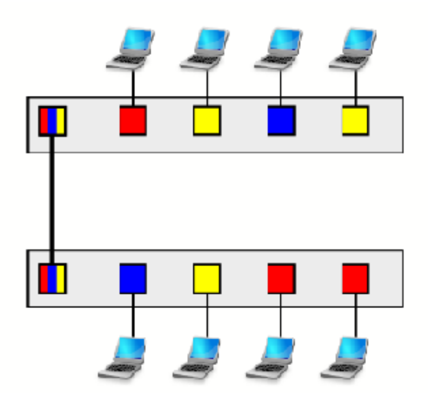
- **Normal Range** تبداء من رقم **1** إلى **1005** هذا اخرى رقم تاخذه آخر شبكة بمعنى يبداء عد الشبكة من الرقم الأول لحد رقم **1005** هذه رقم الشبكة الاخيرة بمعنى الأن يوجد لدنيا **1005** شبكات في هذه الحالة تم استهلاك كل الارقام الموجودة في شبكة الـ **Vlan** ولو اردنا أن نقوم بعمل شبكة اخرى لا نستطيع لي لأنه لا يوجد رقم للشبكة نستطيع اخذه لعمل شبكة جديد , وقد تم حل هذه المشكلة عن طريق توسيع عدد الشبكات و إضافة رنج اكبر من السابقة يسمى **Extended Range** تبداء من رقم **1006** إلى **4096** هذا رقم آخر شبكة تم اخذه و من المستحيل أن نوصل لهذا العدد من الشبكات ولكن تم تطويره و توسيع هذه الاعداد لو في حال نريد إضافة شبكات اخرى سيكون العدد مفتوح لحد **4096** هذه اخرى شبكة ستكون لدنيا .

Vlan Switch Port Modes

عملية ربط المنافذ بشبكة الـ Vlan

- يوجد نوعان من طريقة الربط الطريقة اليدوية و الطريقة الديناميكية .

1- **Static Vlan Port**
2- **Dynamic Vlan Port**



Static Vlan Port : هذه الطريقة اليدوية التي تعتمد على مهندس الشبكة أن يقوم بربط المنفذ بشبكة الـ **Vlan** بشكل يدوي , بمعنى إنه عندما يقوم ببناء شبكة الـ **Vlan** سيقوم بتقسيم المنافذ على الشبكة بشكل يدوي كما يريد .

Dynamic Vlan Port : هذه الطريقة الاتوماتيكية التي تعتمد على إضافة المنافذ المتصلة فيها أجهزة الحاسوب و تعتمد هذه الطريقة على الماك ادرس الخاص في جهاز الحاسوب ليتم الإضافة في شبكة **Vlan**.

أنواع منافذ شبكة الـ Vlan

Vlan Port Type

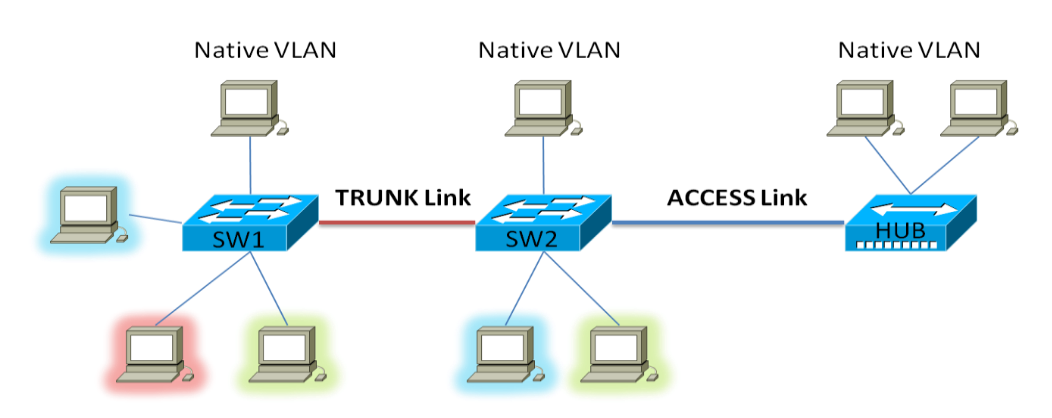
- يوجد نوعان من منافذ شبكة الـ **Vlan** يتم استخدام كل واحد على حسب الوظيفة التي سيعمل فيها سأقوم بذكر الأنواع و شرحهم .

1- Access Port , 2- Trunk Port

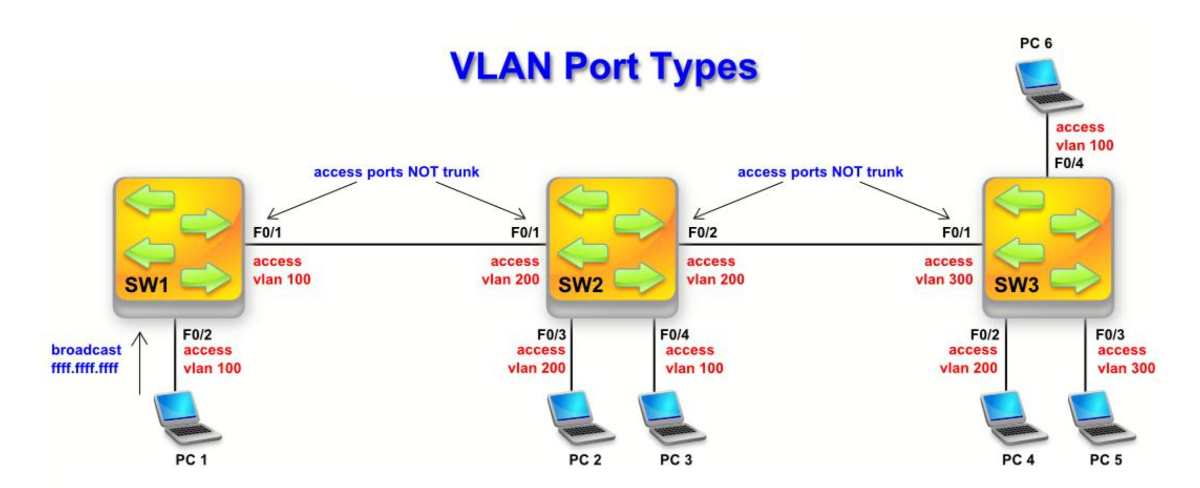
١- **Access Port :** هذا النوع من التوصيل يستخدم في توصيل جهاز مع سويتش و يعتمد هذا النوع على شبكة الـ **Native Vlan** .

٢- **Trunk Port :** هذا النوع من التوصيل يستخدم في توصيل جهاز سويتش مع جهاز سويتش اخر أو جهاز سويتش مع جهاز راوتر ويستخدم هذه التوصيل للتعامل مع البيانات التابعة لأكثر من شبكة **Vlan** و يتم التفريق فيما بين الـ **Frame** التابعة لشبكة **Vlan** مختلفة عن طريق بروتوكول الـ **Trunk** .

- مثال على منفذ الـ **Trunk Port :** لو كان لدينا شبكة مكونة من سوتشين و تم تقسيم شبكة **Vlan 1** على السويتش الأول و قمنا بتقسيم شبكة الـ **Vlan 1** مره اخرى على السويتش الثاني في هذه الحالة تتوجد شبكة الـ **Vlan 1** على سوتشين و نحتاج الداتات أن تنتقل من السويتش الأول للسويتش الثاني , من الطبيعي جداً سنحتاج بروتوكول الـ **Trunk** و سنقوم بتفعيله على منافذ السويتشن لتتم عملية نقل الدتا بشكل صحيح و مع العلم لو كان يوجد اكثر من شبكة **Vlan** سيتم تفريق الداتا مرسلة لأي شبكة من هذه الشبكات عن طريق بروتوكول الـ **Trunk** ليتم وصول الداتا للشبكة المطلوبة , كما في النموذج التالي :



أنظر للنموذج هذا مفهوم اكثر للمثال السابقة



- لاحظ إنه تم التوصيل ما بين السويتشات ربط الـ **Trunk Port** لي لأنه يوجد في **SW2** و **SW3** نفس شبكة الـ **Vlan 200** و نريد أن تنتقل المعلومات و الداتا لهذه الشبكة سنقوم برط و توصيل الـ **Trunk Port** ليتم التفريق و التوصيل ما بين الداتا لكل شبكة **Vlan** .

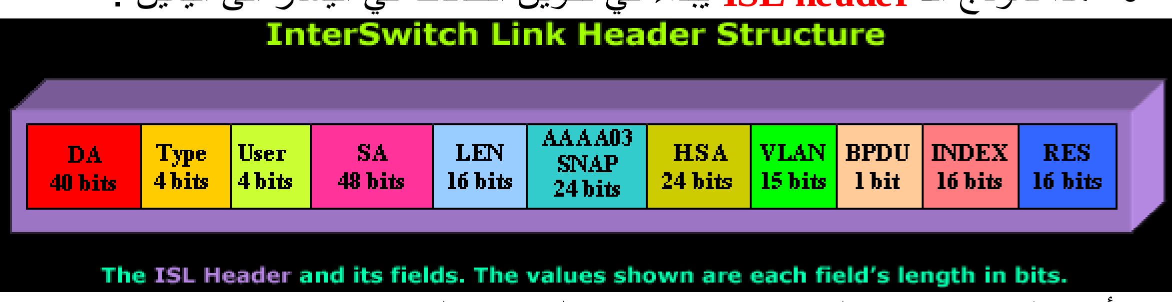
أنواع البروتوكولات المستخدمة في Trunk Port

- يوجد نوعان يتم الاعتماد عليهما في عملية تغليف و إرسال الـ **Frame** في عملية توصيل منفذ الـ **Trunk Port** سأقوم بذكرهم و شرحهم .

1- Inter-Switch Link (ISL) , 2- IEEE 802.1Q

Inter-Switch Link (ISL) : هو عبارة عن بروتوكول خاص بشركة سيسكو و هذا البروتوكول يقوم بعملية تغليف الـ **Frame**, ولكن قبل بداية تغليف الـ **Frame** يبداء في تكوين **ISL header** المكون من عدة خانات و يصل طول هذا الـ **ISL header 26 byte** و يتم إضافة المعلومات الخاصة في كل شبكة **Vlan** في كل خانة على حسب مكان المعلومات المناسب في الخانات.

- هذا نموذج الـ **ISL header** يبداء في تكوين الخانات في اليسار الى اليمين .



- سأقوم بذكر محتويات الـ **ISL header** و التعرف عليهم و شرحهم .

- DESTINATION ADDRESS (DA) FIELD
- TYPE FIELD
- USER DEFINED FIELD

- SOURCE ADDRESS (SA) FIELD
- LENGTH FIELD
- AAAA03 (SNAP) FIELD
- HIGH BITS SOURCE ADDRESS (HSA) FIELD

- VLAN - DESTINATION VIRTUAL LAN ID FIELD
- BPDU FIELD
- INDEX FIELD
- RES FIELD

- الأن سأقوم بشرح كل الخانات بشكل منفرد عن الآخر لنستطيع فهم كل خانة ما هي الوظيفة التي تعمل فيها و ما هي البيانات التي تحتويها هذه الخانات .

- **DESTINATION ADDRESS (DA) FIELD :** هذه الخانة طولها **40 bits** فهي تحتوي على العنوان المطلوب الماك ادرس, الذي نريد الإرسال اليه و يقوم ايضاً بعملية الإرسال المستهدف مثل يرسل بشكل متتعد لمجموعة عناوين مرة واحدة.

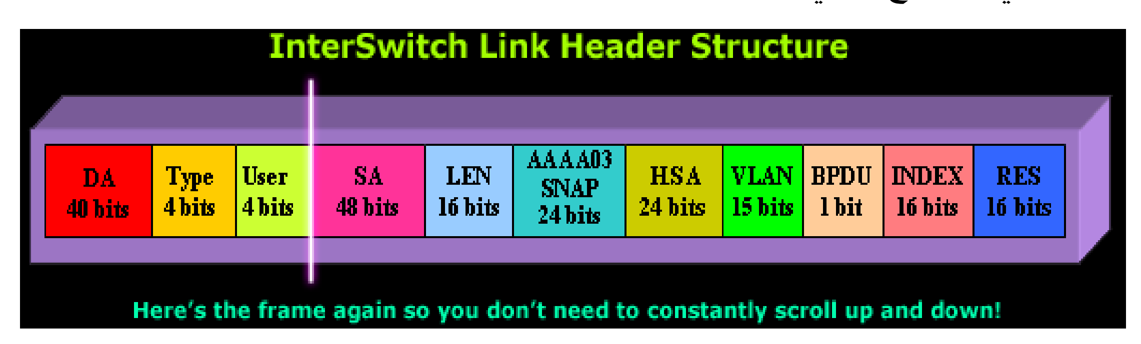
- **TYPE FIELD :** هذا الحقل طوله **4 bits** وظيفة هذه الخانة تقوم بتميز الإطار

- الاصلي الذي تم تغليفها إعتماد على نوع الإطار, و يوجد اكثر من قيمة ليتم الاعتماد عليها في عملية التغليف على حسب النوع المطلوب .

Type Value	Encapsulated Frame
0000	Ethernet
0001	Token-Ring
0010	FDDI
0011	ATM

- USER DEFINED FIELD : هذه الخانة طولها ايضاً **4 bits** هذه الخانة تعتمد على الخانة الأولى و تعتمد ايضاً على عملية التغليف الاصلية التي ستكون **Ethernet**.

- الأن تم شرح القسم الأول من الخانات التي في القسم الأول من بناء الـ **ISL header** كما في النموذج التالي :



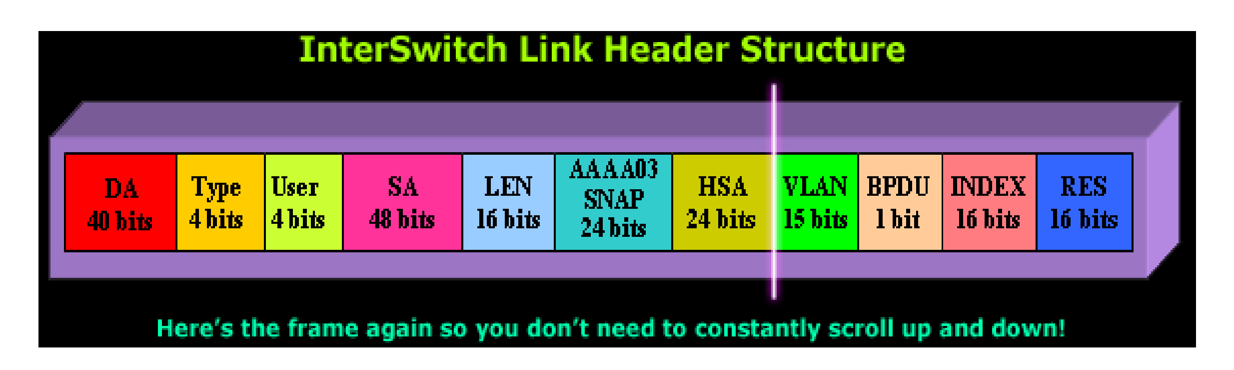
- الأن سنبداء في شرح القسم الثاني من الخانات :

- SOURCE ADDRESS (SA) FIELD : هذا الخانة التي تحتوي على عنوان الملك ادرس الخاص في جهاز المرسل **Source MAC Address** و معرفة المنفذ الذي سيتم الإرسال منه الـ **Frame** , و هذه الخانة طولها **48 bits** .

- LENGTH FIELD : هذه الخانة طولها **16 bits**

- HIGH BITS SOURCE ADDRESS (HSA) FIELD :

- الأن تم شرح القسم الثاني من الخانات التي في القسم الثاني من بناء الـ **ISL header** كما في النموذج التالي :



- الأن سنبداء في شرح القسم الثالث و الاخير من الخانات :

- VLAN - DESTINATION VIRTUAL LAN ID FIELD : هذه الخانة من أهم الخانة طولها **15 bits** وظيفة هذه الخانة هي عملية تحديد رقم الـ **Virtual LAN ID** التي سيتم إرسال المعلومات اليه بينما يتم تنقل هذه البيانات أو الإطار الـ

frame في بروتوكول الـ **trunk** و تكون في داخلها رقم شبكة الـ **VLAN** و العلومات الباقية حيث إنه لا تسلم لشبكة آخرى الا للشبكة التي تنطبق فيها رقم شبكة الـ **VLAN** و هذه الخانة من أهم الخانات الموجودة .

- **BPDU FIELD :** هذه الخانة طولها **1 bit** هذه الخانة تحتوي على بروتوكولات مثل **STP** و **VTP** و **CDP** , وظيفة هذه الخانة مهم جداً و هي تقوم بمنع دوران البيانات في السويتش مثل عندما ترسال الـ **Frame** ستوصل للشبكة المطلوبة ولكن إذا كان هناك عدة سوتيشات متصلة مع بعض عن طريق اكثر من لينك سيتم عودة إرسال هذه الـ **Frame** , مما ينتج عن حدوث دوران في الشبكة **network loops** سأقوم بشرح هذه البروتوكولات في الدروس القادمة .

- **INDEX FIELD :** هذه الخانة هي المسؤولة عن الدليل الخاص في الإطار و عن مصدر الإطار من بداية إرسال ه الى أن يتم وصولها هذه هي وظيفة هذه الخانة, و نستطيع ايضاً أن نراقب الإطار من بداية إرسال ه حتى استلامه .

- **RES FIELD :** هذه الخانة المسؤولة عن حجز نوع الإرسال في الكابل و تحديد نوعه قبل عملية الإرسال و تحديد نوع الشبكة ايضاً هل هي **FDDI** أو **Token Ring** أو **Ethernet** و طول هذه الخانة **16 bits**.

٢- IEEE 802.1Q

هذا البروتوكول يقوم بنفس وظيفة الـ **ISL** ولكن يوجد بعض المميزات التي يتفوق فيه بروتوكول **IEEE 802.1Q** عن بروتوكول الـ **ISL** , مثل بروتوكول الـ **IEEE 802.1Q** يقوم بفقط بعمل **Tag** على الـ Frame بحجم **4 byte** على عكس بروتوكول الـ **ISL** حيث إنه يقوم بعملية الـ **Encapsulation** للـ **Frame** بحجم **26 byte** و هذا الفرق ما بين هذه البروتوكولات و من الافضل استخدام بروتوكول الـ **IEEE 802.1Q** لإنه فقط يقوم بوضع **Tag** على الـ **Frame** و هذا يجعل الـ **Frame** حجمها صغير جداً .

- **ملاحظة : هذا البروتوكول خاص في مؤسسة IEEE و هو غير ملكية لشركة سيسكو و شركة سيسكو تنصح باستخدام هذا البروتوكول بدل من استخدام الـ ISL.**

- **Frame format صيغة الإطار: هي عملية بناء الإطار و لا يقوم بعملية encapsulate كما ذكرنا سابقاً , و هذا النموذج الذي يتكون منه هذا البروتوكول.**

16 bits	3 bits	1 bit	12 bits
TPID	TCI		
	PCP	DEI	VID

- هذا النموذج الذي يتم بناء الخانات عليه لبروتوكول الـ **IEEE 802.1Q** .
و بهذا الشكل نكون قد تم الانتهاء من الشرح بشكل كامل و سنبداء في الدرس العملي و التطبيق .

إعدادات شبكة الـ Vlan Switch

Vlan Configuartion

Switch > **enable**

Switch # **config t**

Switch (config) # **vlan 2**

Switch (config-vlan) # **name IT** ← أسم الشبكة

Switch (config-vlan) # **exit**

Switch (config-vlan) # **vlan 3**

Switch (config-vlan) # **name PMP** ← أسم الشبكة

Switch (config-vlan) # **exit**

Switch (config) # **interface fastethernet 0/1**

Switch (config-if) # **switchport access vlan 2**

Switch (config-if) # **exit**

Switch (config) # **interface fastethernet 0/7**

Switch (config-if) # **switchport access vlan 3**

Switch (config-if) # **exit**

Switch (config) # **exit**

Switch # **copy running-config startup-configt**

- سنقوم بعمل شبكة مكونة من جهازين سوتيش و سنقوم بتقسيم شبكات الـ **Vlan** على السويتشات , و سنقوم بتعرف على إعدادات الشبكة :
- في البداية سنقوم بتطبيق العملي على الطوبولوجي المكون من شبكتين **Vlan** مقسمية على جهازين سويتش و يربط ما بينهم لينك **Trunk Port** الذي قمنا بشرح سابقاً .

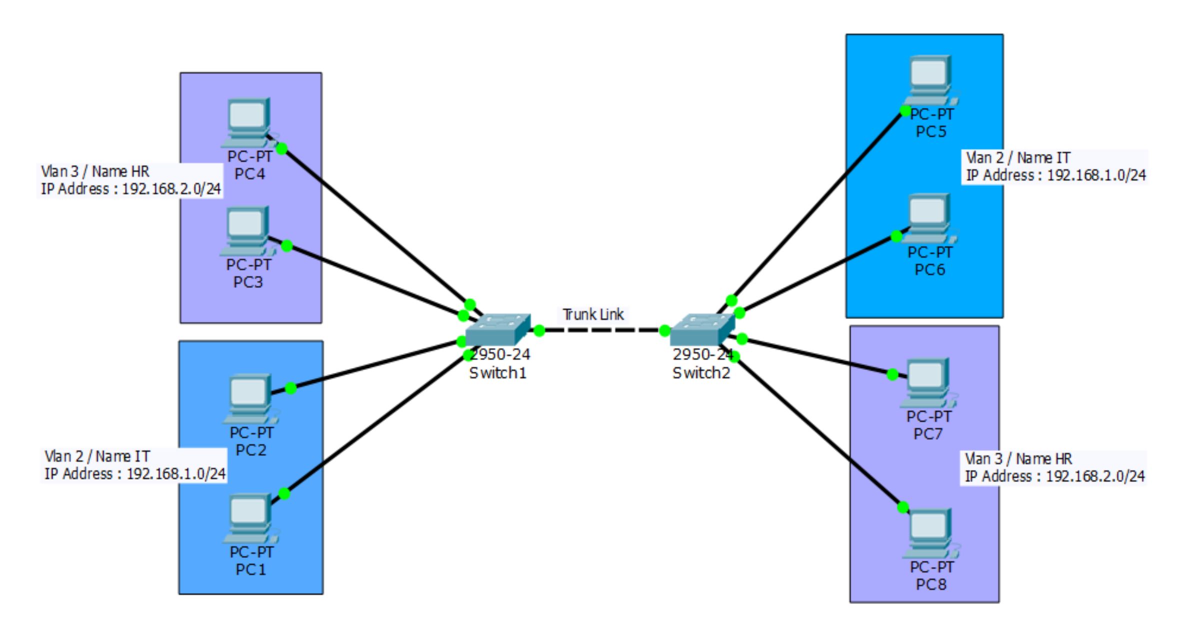
- **إعدادات الشبكة :**

١- الشبكة الأولى ستكون بعنوان **192.168.1.0/24** هذا عنوان الشبكة الأولى و التي ستاخذ رقم شبكة الـ **Vlan 2** و اسم الشبكة **Name IT** .

٢- الشبكة الثاني ستكون بعنوان **192.168. 2.0/24** هذا عنوان الشبكة الثانية والتي ستاخذ رقم الشبكة **Vlan 3** و اسم الشبكة **Name HR** .

٣- سنقوم بتركيب عنوان الاي بي على كل الاجهز الحاسوب على حسب ترتيب الشبكة المنتمي اليه أجهزة الحاسوب .

صورة النموذج الذي سيتم العمل عليه



- الأن بعد أن تعرفنا على الشبكات و الإعدادات سنقوم بعمل إعدادات الشبكات بدخول على السويتشات و انشاء الـ **Vlan** و تقسيم الإنترفيس على كل شبكة من شبكة الـ **Vlan** كما في النموذج السابق .

- **ملاحظة مهم جداً :** قمنا بعمل شبكة الـ **Vlan 2** هذه يدل على إنه شبكة **Vlan 1** موجودة ولكن لا نستطيع استخدامها لي لأنه محجوزة في داخل السوتيش و هي الشبكة التي تحتوي على جميع المنافذ الموجودة على السوتيش , و من شبكة **1002 , 1003** , **1004 , 1005** ايضاً هذه الشبكة محجوزة ولا يمكن أن نستخدمها في العمل لي لأنه محجوزة في داخل السوتيش لبعض الاعمل الآخر مثل ما هو متواجد في النموذج التالي يوضح لنا ما قمنا بشرحه .

الشبكات المحجوزة في داخل السويتش أنظر للصورة التالي

```
VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                Fa0/21, Fa0/22, Fa0/23, Fa0/24
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup
```

- الأن سنقوم بدخول على الـ **SW 1** و عمل الإعدادات التالية :

الأن سنقوم بكتابة الأوامر التالية :

Switch> **enable**

Switch # **config t**

Switch (config) # **vlan 2**

Switch (config-vlan) # **name IT**

Switch (config-vlan) # **exit**

Switch (config) # **interface fastethernet 0/1**

Switch (config-if) # **switchport access vlan 2**

Switch (config-if) # **exit**

Switch (config) # **interface fastethernet 0/2**

Switch (config-if) # **switchport access vlan 2**

Switch (config-if) # **exit**

Switch (config) # **vlan 3**

Switch (config-vlan) # **name HR**

Switch (config-vlan) # **exit**

Switch (config) # **interface fastethernet 0/3**

Switch (config-if) # **switchport access vlan 3**

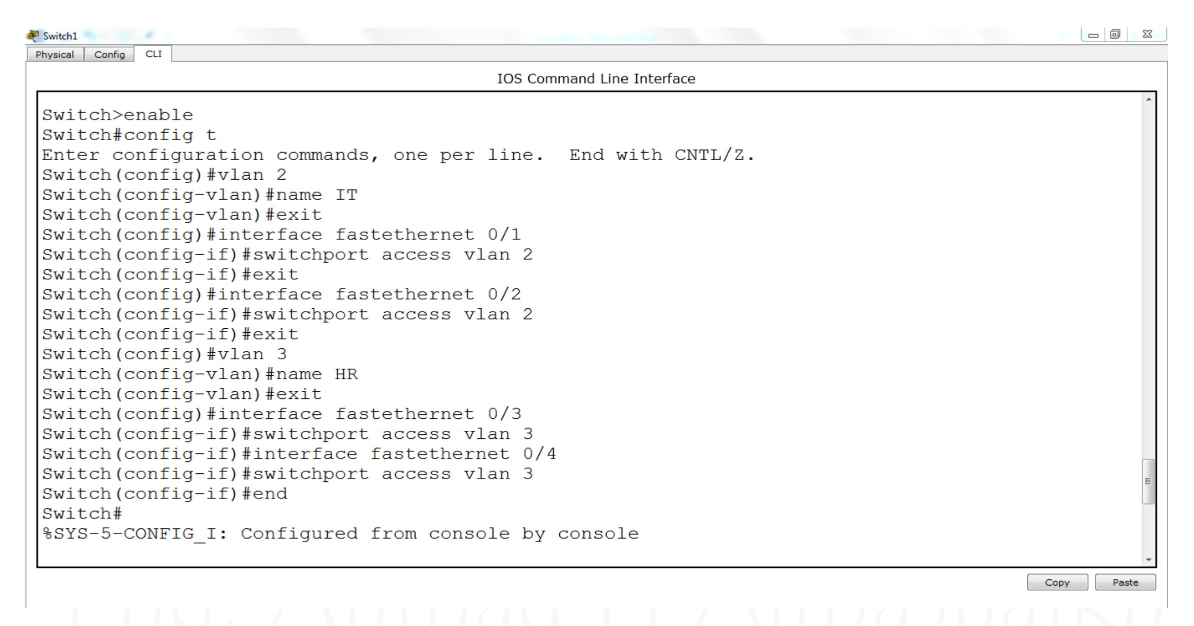
Switch (config-if) # **interface fastethernet 0/4**

Switch (config-if) # **switchport access vlan 3**

Switch (config-if) # **end**

Switch # **copy running-config startup-config**

كما في الصورة التالية من داخل SW 1

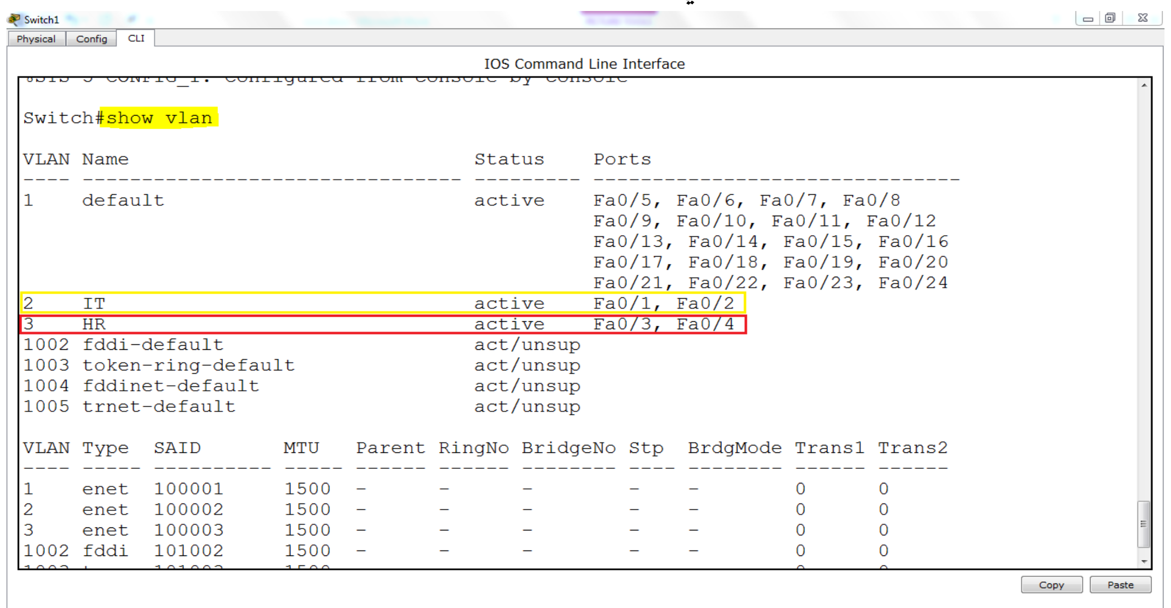


```
Switch>enable
Switch#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#vlan 2
Switch(config-vlan)#name IT
Switch(config-vlan)#exit
Switch(config)#interface fastethernet 0/1
Switch(config-if)#switchport access vlan 2
Switch(config-if)#exit
Switch(config)#interface fastethernet 0/2
Switch(config-if)#switchport access vlan 2
Switch(config-if)#exit
Switch(config)#vlan 3
Switch(config-vlan)#name HR
Switch(config-vlan)#exit
Switch(config)#interface fastethernet 0/3
Switch(config-if)#switchport access vlan 3
Switch(config-if)#interface fastethernet 0/4
Switch(config-if)#switchport access vlan 3
Switch(config-if)#end
Switch#
%SYS-5-CONFIG_I: Configured from console by console
```

- بهذا الشكل نكون قد قمنا بعمل الإعدادات الخاصة في شبكة **vlan 2** و **vlan 3** و قمنا بتحديد و تقسيم المنافذ على الشبكة و سنقوم باستعراض الشبكة الموجودة و التي تم تقسيمها سنقوم بكتابة الأمر التالي :

Switch # **show vlan**

كما في الصورة التالية

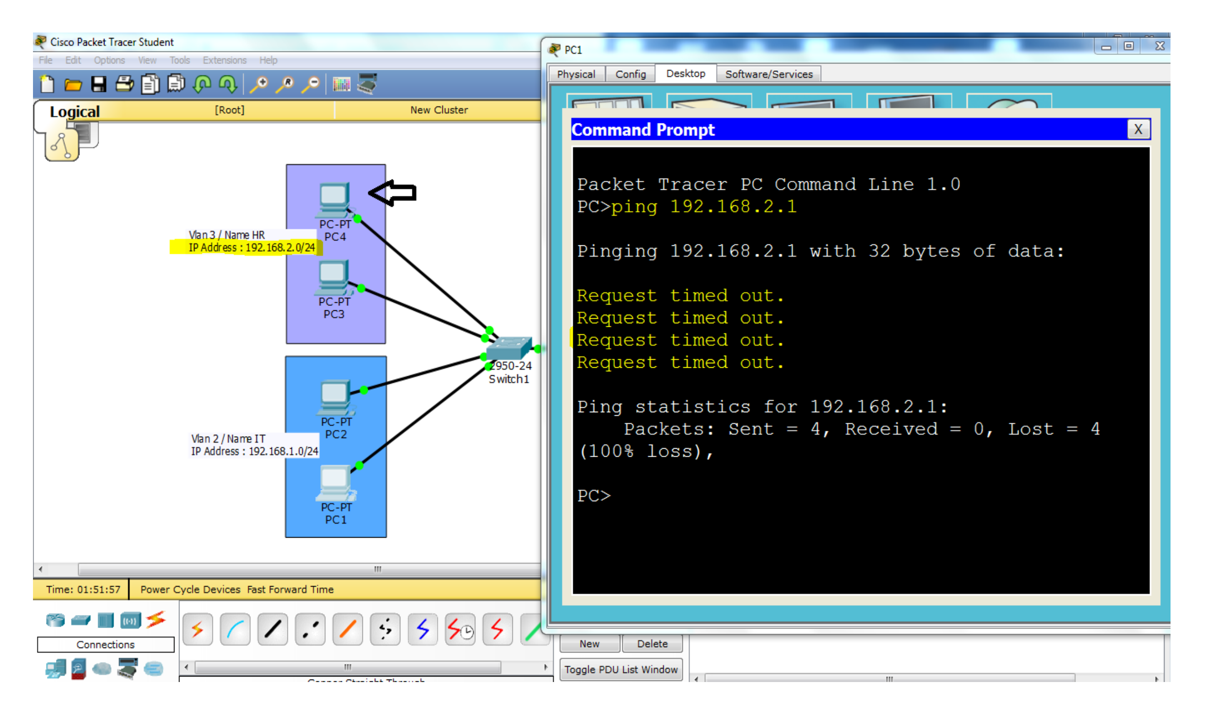


```
Switch#show vlan

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                Fa0/21, Fa0/22, Fa0/23, Fa0/24
2    IT                               active    Fa0/1, Fa0/2
3    HR                               active    Fa0/3, Fa0/4
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
1    enet  100001     1500  -      -      -        -    -        0      0
2    enet  100002     1500  -      -      -        -    -        0      0
3    enet  100003     1500  -      -      -        -    -        0      0
1002 fddi  101002     1500  -      -      -        -    -        0      0
```

- سنرى إنه يوجد شبكة **vlan 2** و **vlan 3** تاخذ الاسماء التي قمنا بتمسية الشبكات بهم و كل شبكة تساوي المنافذ التي قمنا بتعينهم للشبكة , في هذه الحالة شبكة **vlan 2** لا تستطيع الاتصال بشبكة **vlan 3** لي لأنه تم فصلهم عن بعضهم البعض و تم تقسيم المنافذ و تركيب العناوين عليهم بشكل مختلف عن الآخر سنقوم بعمل اختبار ما بين الشبكات لنرى هل سيتم الاتصال أو لا تابع التالي ...
- سنقوم بعمل اختبار عن طريق امر الـ **Ping** سنقوم بعملية اتصال من شبكة الـ **vlan 2** للـ **vlan 3** و نرى هل سيتم الاتصال أو الرد أو لا , سنقوم بدخول على أحد أجهزة الحاسوب الموجودة في شبكة الـ **vlan 2** و نقوم بدخول على الـ **Command Prompt** و نقوم بكتابة التالي لنرى هل يستطيع الاتصال في الجهاز الموجود في شبكة الـ **vlan 3** أو لا لنرى .



- لاحظ في الصورة تم الرد برسالة **. Request timed out** هذه الرسالة تعني إنه لا يستطيع الاتصال ولا يوجد رد من الجهاز الموجود في شبكة الـ **vlan 3** يجب أن نعرف إنه في هذه الحالة الشبكات تعمل بشكل صحيح و تم فصلهم عن بعضهم البعض و إذا اردنا الشبكات أن تستطيع الاتصال مع بعضها البعض نحتاج لجهاز الراوترات لربط الشبكات مع بعضهما البعض .

- الأن بعد الانتهاء من هذه الإعدادات على الـ **SW 1** سنقوم بدخول على الـ **SW 2** لنقوم بنفس الإعدادات عليه و بناء نفس الشبكات و سنرى كيف سيتم الاتصال ما بين السويتشات عن طريق وصلة الـ **Trunk** .

- الأن سنقوم بدخول على الـ **SW 2** و عمل الإعدادات التالية :

الأن سنقوم بكتابة الاوامر التالية :

Switch> **enable**

Switch # **config t**

Switch (config) # **vlan 2**

Switch (config-vlan) # **name IT**

Switch (config-vlan) # **exit**

Switch (config) # **interface fastethernet 0/1**

Switch (config-if) # **switchport access vlan 2**

Switch (config-if) # **exit**

Switch (config) # **interface fastethernet 0/2**

Switch (config-if) # **switchport access vlan 2**

Switch (config-if) # **exit**

Switch (config) # **vlan 3**

Switch (config-vlan) # **name HR**

Switch (config-vlan) # **exit**

Switch (config) # **interface fastethernet 0/3**

Switch (config-if) # **switchport access vlan 3**

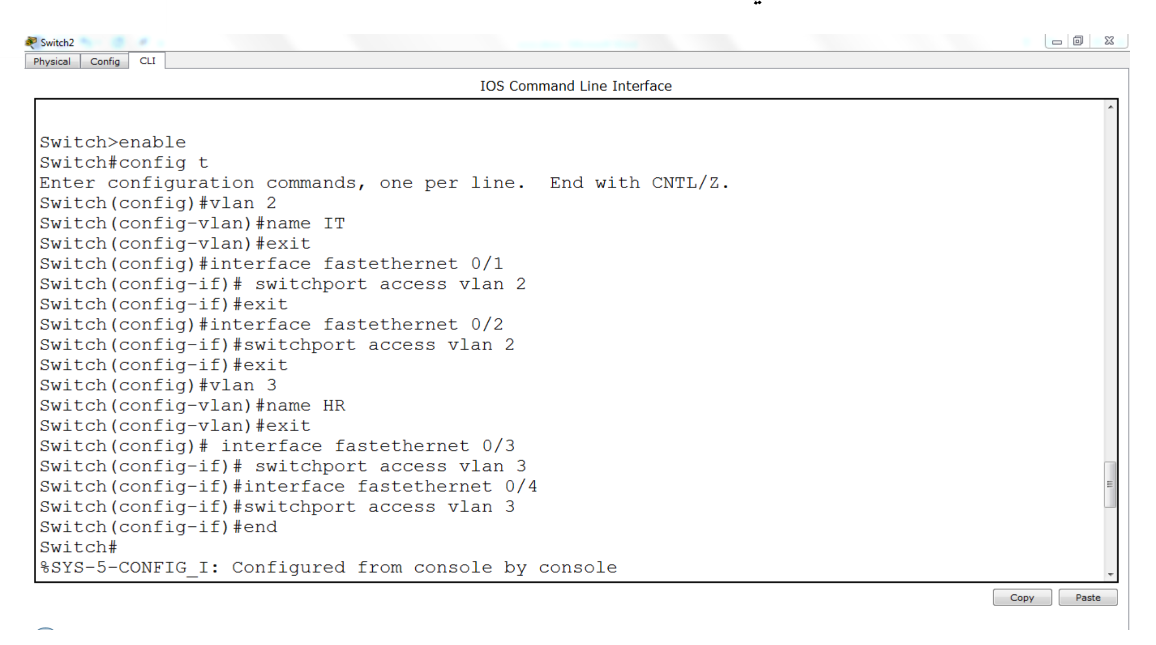
Switch (config-if) # **interface fastethernet 0/4**

Switch (config-if) # **switchport access vlan 3**

Switch (config-if) # **end**

Switch # **copy running-config startup-config**

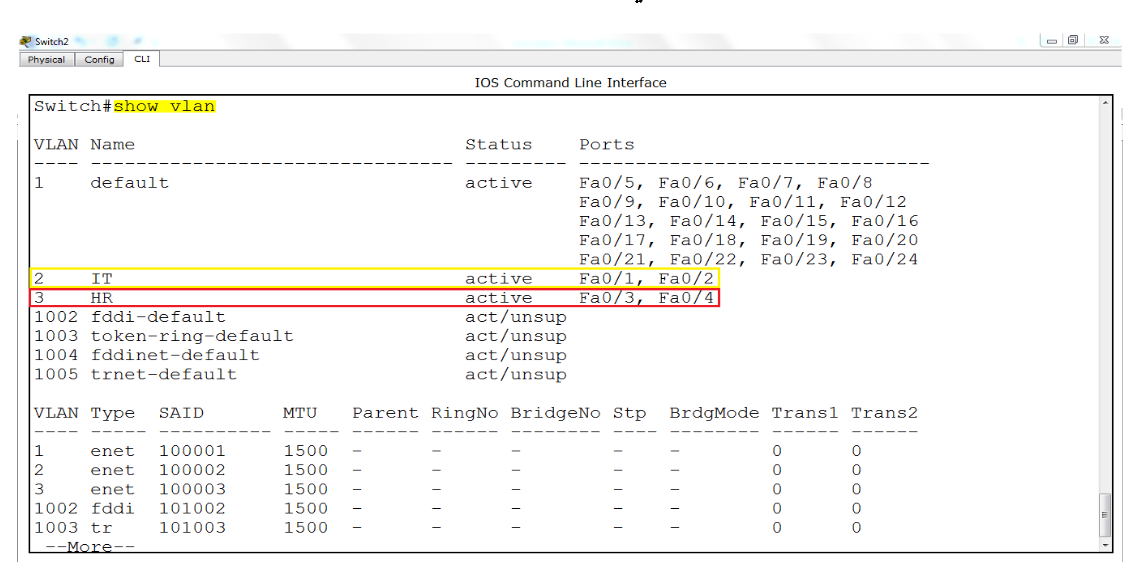
كما في الصورة التالية من داخل SW 2



- بهذا الشكل نكون قد قمنا بعمل الإعدادات الخاص في شبكة **vlan 2** و **vlan 3** و قمنا بتحديد و تقسيم المنافذ على الشبكة و سنقوم باستعراض الشبكة الموجودة و التي تم تقسيمها سنقوم بكتابة الأمر التالي :

Switch # **show vlan**

كما في الصورة التالية



- سنرى إنه يوجد شبكة **vlan 2** و **vlan 3** تاخذ الاسماء التي قمنا بتمسية الشبكات بهم و كل شبكة تساوي المنافذ التي قمنا بتعينهم للشبكة , في هذه الحالة شبكة **vlan 2** لا تستطيع الاتصال بشبكة **vlan 3** لي لأنه تم فصلهم عن بعضهم البعض و تم تقسيم المنافذ و تركيب العناوين عليهم بشكل مختلف عن الآخر , في هذه الحالة تم إضافة الشبكات في **SW 2** و **SW 1** ولكن لا تستطيع الاتصال مع بعضهم البعض الشبكات

حتى ولو كانو بنفس الشبكة و نفس العنوان وذالك لي إنه تم ربط السويتشات من خلال **Trunk** و هذه النوع من الربط يحتاج لعمل بعض الإعدادات ليتم الاتصال و تنقل البيانات ما بين الشبكات من خلال هذا الربط سنقوم الأن بعمل الإعدادات الخاص في منفذ الـ **Trunk** تابع .

- الأن سنقوم بدخول على الـ **SW 1** و عمل الإعدادات التالية :

الأن سنقوم بكتابة الاوامر التالية :

Switch> **enable**

Switch # **config t**

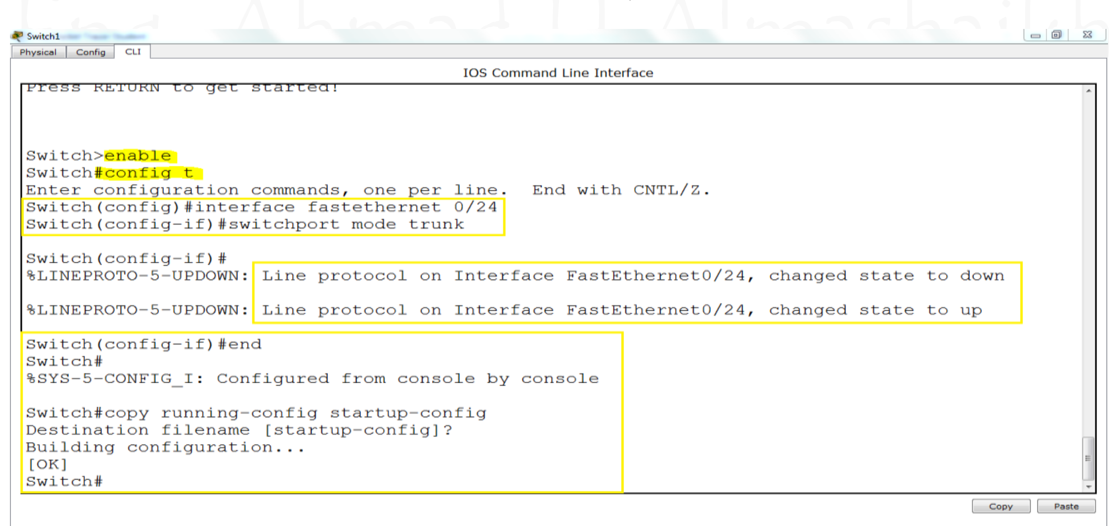
Switch (config) # **interface fastethernet 0/24**

Switch (config-if) # **switchport mode trunk**

Switch (config-if) # **end**

Switch # **copy running-config startup-config**

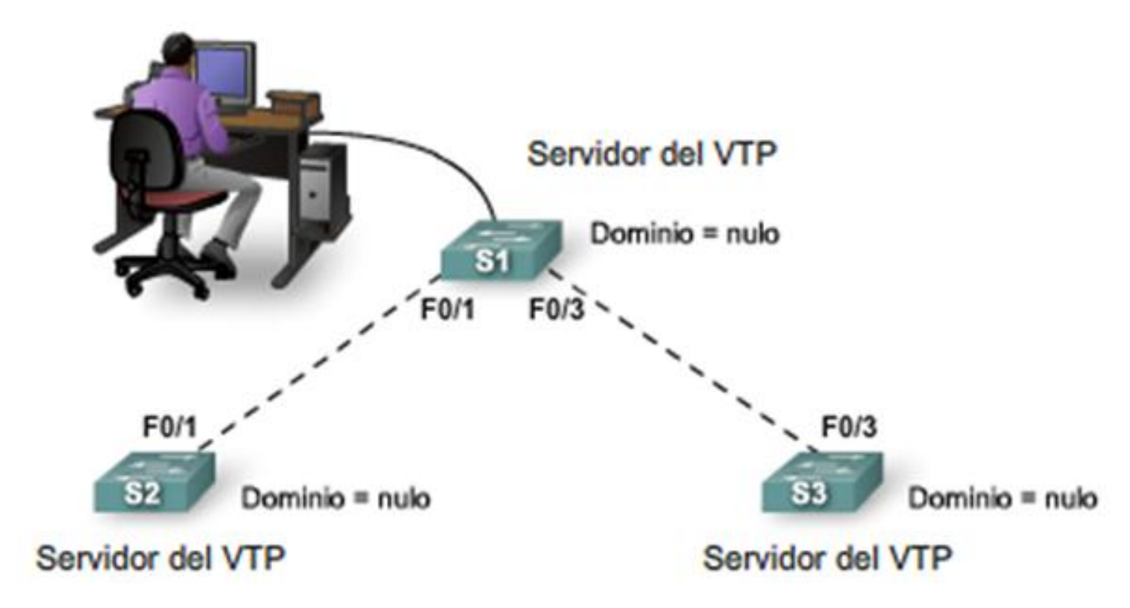
كما في الصورة التالية



- لاحظ إنه بعد كتابة الأمر **switchport mode trunk** تم ايقاف **down** و اعادة تشغيل **up** الإنترفيس مرة اخرى ليتم تفعيل الأمر بشكل صحيح , و بهذا الشكل نكون قد تم الانتهاء من إعدادات المنفذ .

- **ملاحظة :** عندما نقوم بتفعيل بروتوكول الـ **trunk** على أحد المنافذ الخاصة في السويتش الأول سيتم بشكل اوتوماتيكي تفعيل المنفذ الثاني المرتبط فيه بسويتش الثاني.
- بهذا الشكل تسطيع الشبكات التي مرتبطة في **SW 2** أن تتصل في الشبكة المرتبطة في الـ **SW 1** عن طريق منفذ الـ **trunk** .

VTP
VLAN Trunk Protocol



VTP : هو عبارة عن بروتوكول خاص في شركة سيسكو و هذا البروتوكول يعمل على أجهزة السويتشات، و فكرة الـ **VTP** إنه يقوم بإنشاء شبكات الـ **Vlan** بطريقة اتوماتيكية على باقي السويتشات التي عليه نفس شبكة الـ **Vlan**، مثل عندما ا يكون لدينا اكثر من سويتش في الشبكة و تم عمل إعدادات شبكة الـ **Vlan** على جهاز سويتش واحد و بدل من أن نقوم بتكرير نفس الإعدادات على باقي السويتشات سنقوم بتفعيل بروتوكول الـ **VTP** ليقوم بإنشاء الشبكات على باقي السويتشات بشكل اتوماتيكي من غير أن نقوم بنفس الإعدادات على باقي السويتشات سيتم تبادل هذه الشبكات ما بين السويتشات عن طريق المنفذ الذي سيكون **Trunk port** ليتم تنقل الـ **Frame** ما بين السويتشات .

- نستطيع أن نقول بروتوكول الـ **VTP** هو عبارة عن بروتوكول يقوم بأدارة شبكة الـ **Vlan** على السويتشات الموجودة في نفس الدومين بمعنى تكون تحت نطاق واحد ، ويجب أن نعرف إنه لا يقوم بعمل **Vlan** جديدة في السويتشات بلا يجب أن نعرف إنه يقوم بعمل نفس شبكة الـ **Vlan** الموجودة في السويتشات الأولى بمعنى إنه يقوم بعمل نسخ للشبكات ، و يفيد ايضاً في عملية الصيانة مثل عندما نريد حذف شبكة أو إضافة شبكة أو التعديل على شبكة سنقوم بتعديل مره واحدة على السويتش الذي سيكون الرئيسي في الشبكة و هو يقوم بتعديل و على باقي السويتشات الموجودة و سأقوم بذكر و بشرح أنواع الـ **VTP** .

- **VTP Mode:** هي عبارة عن حالة بروتوكول الـ **VTP** التي يعتمد عليه السويتش و يوجد ثلاث مستويات من هذه الحالة سأقوم بذكرهم و شرحهم و متى يتم استخدام كل نوع من هذه الانواع.

أنواع VTP Mode

1- **VTP Server الخادم**

2- **VTP Client المضيف**

3- **VTP Transparent الوسيط ما بين الـ Client و Server**

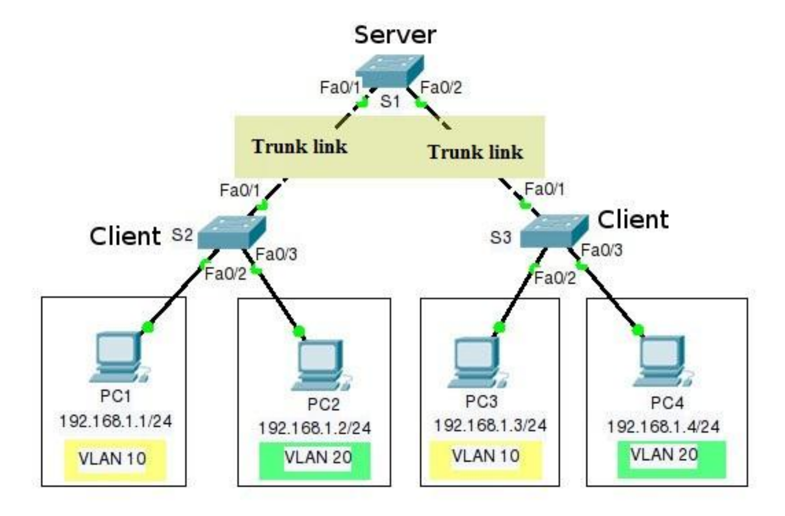
- **الأن بعد أن تعرفنا على الأنواع سأقوم بشرحهم :**

١- **VTP Server :** هذا النوع هو الذي سيكون السويتش الرئيسي بمعنى إنه الخادم الذي سيقوم بادارة و انشاء الـ **VTP Domain** وكذالك هو المسؤولة عن السويتشات التي تتشارك في نفس قاعدة البيانات الخاصة في شبكة الـ **Vlan** و جميع السويتشات التي ستشارك شبكة الـ **Vlan** ستكون تحت هذا السويتش الرئيسي ليتم إرسال و استقبال التحديثات و التغيرات.

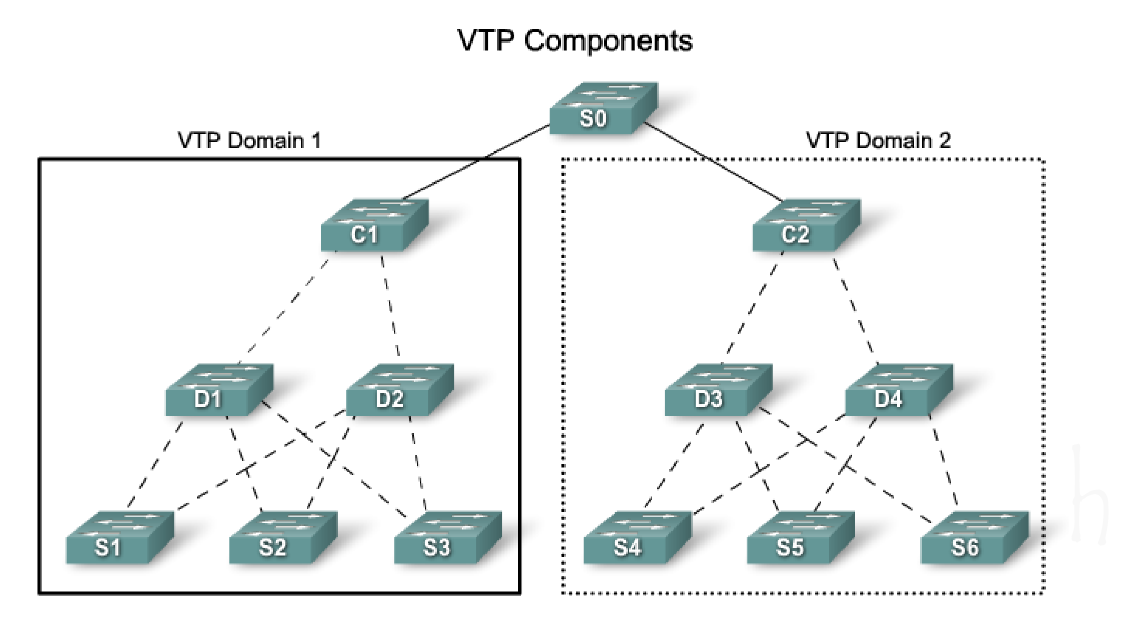
٢- **VTP Client :** هذا النوع سيكون السويتش المستقبل التحديثات و البيانات و الشبكات من السويتش الرئيسي ، ويجب أن نعرف أن هذا النوع هو فقط يستقبل المعلومات و التغيرات و التحديثات و يقوم فقط بتقديم الخدمة ولكن لا يستطع أن يحذف أو يعدل أو يضيف شبكة من شبكات الـ **Vlan**، بمعنى إنه فقط من يتسطيع التعديل و الحذف و التغير هو السويتش الرئيسي فقط لا غير .

٣- **VTP Transparent :** هذا النوع الذي سيتم استخدامه في عملية نقل المعلومات و التحديثات الخاص في بروتوكول الـ **VTP** في ما بين السويتشات التي تعمل **VTP Server** و **VTP Client** و نحتاج هذا النوع في حالة نادرة جداً جداً ولكن الاكثر استخداماً هو الـ **VTP Server** و **VTP Client**.

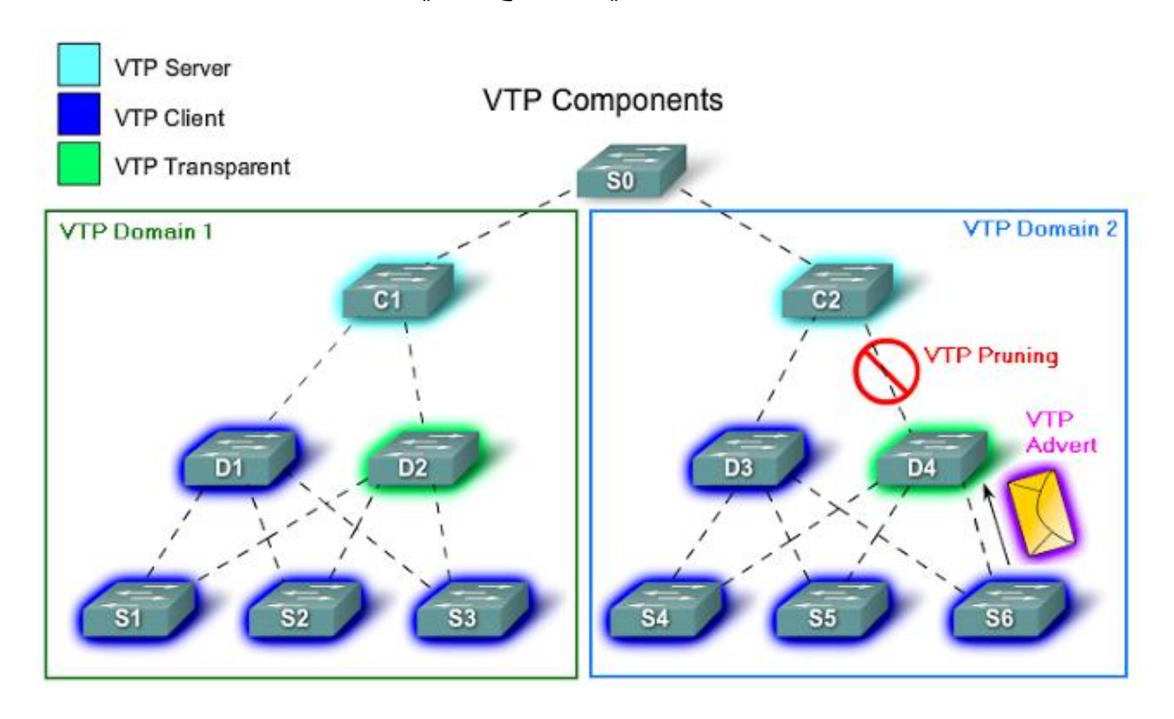
كما في النموذج التالي



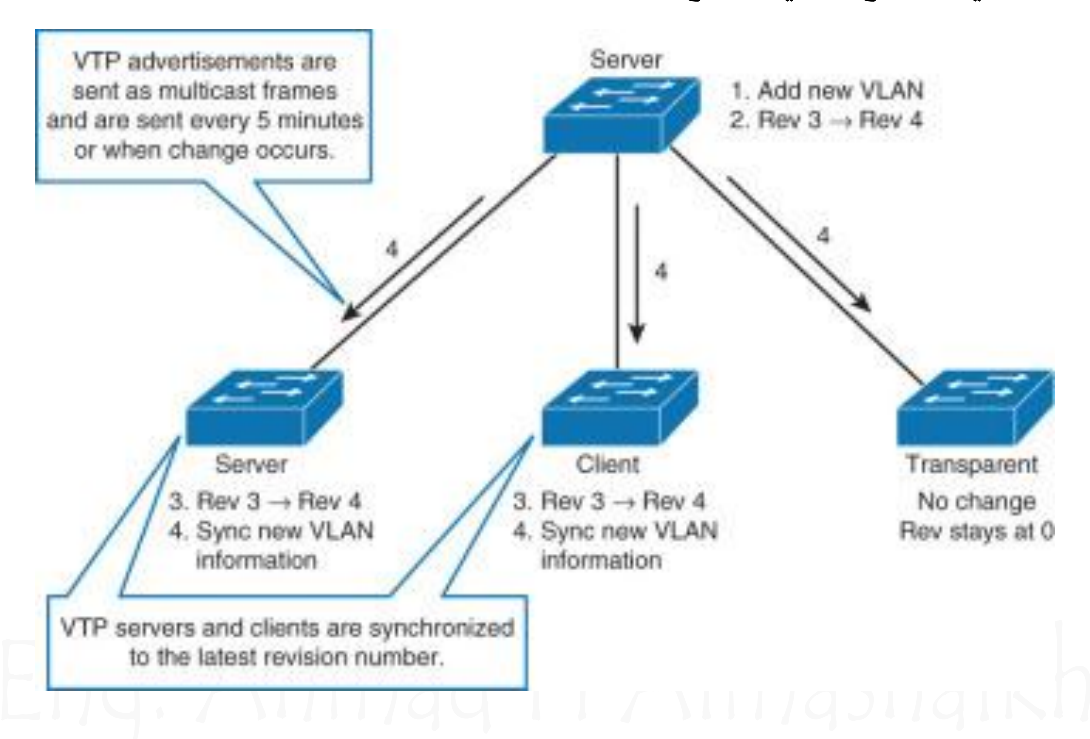
- **VTP Domain** : فكرة هذه الخدمة هي أن تقوم بتنظيم جميع السويتشات تحت نطاق واحد بأسم نطاق معين و تفيد ايضاً عندما نقوم بعمل اكثر من شبكة و تكون هذه الشبكة تم عملها على اكثر من سويتش في نفس الشبكة و نفس النطاق سنقوم بتفعيل هذه الخدمة و تسمية النطاق كما نريد لتكون جميع السويتشات في نطاق واحد و العمل في داخل نطاق واحد ، ويجب أن نكون على معرفة إنه جميع السويتشات ستكون تعمل في بروتوكول الـ **VTP** ، كما في النموذج التالي يوجد لدينا نطاقين **VTP Domain 1** و **VTP Domain 2** في هذه الحالة يجب أن نكون قد فهمنا ما معنى **VTP Domain** .



- **VTP Pruning** : هذه العملية تستخدم في حالة نريد ايقاف منفذ معين من إرسال البيانات و التحديثات لسويتش معين كما في النموذج التالي.



- **VTP Advertisements**: هذه العملية المسؤولة عن الاعلان الذي يحدث في السويتشات مثل عندما يحدث تغير أو تعديل أو انشاء أو حذف شبكة أو تحديث معلومات، ستقوم هذه العملية بإرسال جميع التغيرات التي حدثة في السويتش الرئيسي للسويتشات الآخر ليتم التعديل عليهم و تكون على تحديث مباشر مع السويتش الرئيسي كما في النموذج التالي يوضح العملية.



مكونات عملية الاعلان VTP Advertisements

VTP advertisements send this global domain information:

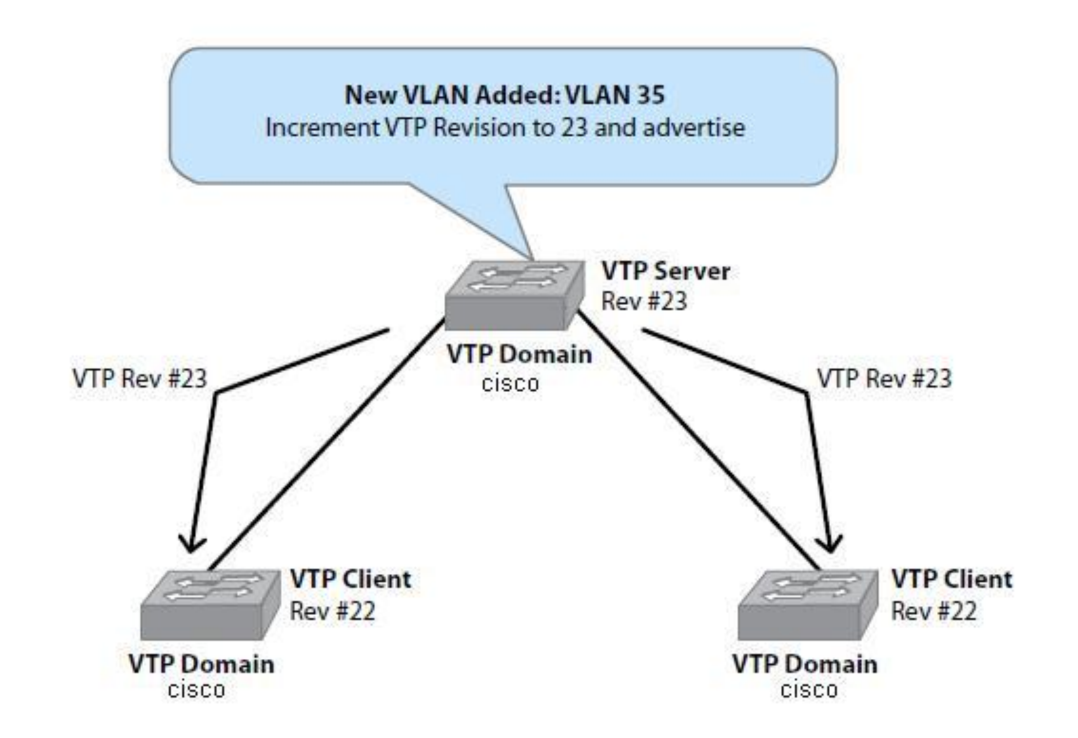
- VTP domain name
- Updater identity and update timestamp
- MD5 digest
- Frame format

VTP advertisements send this VLAN information:

- VLAN ID
- VLAN name
- VLAN type
- VLAN state
- Additional VLAN configuration information specific to the VLAN type

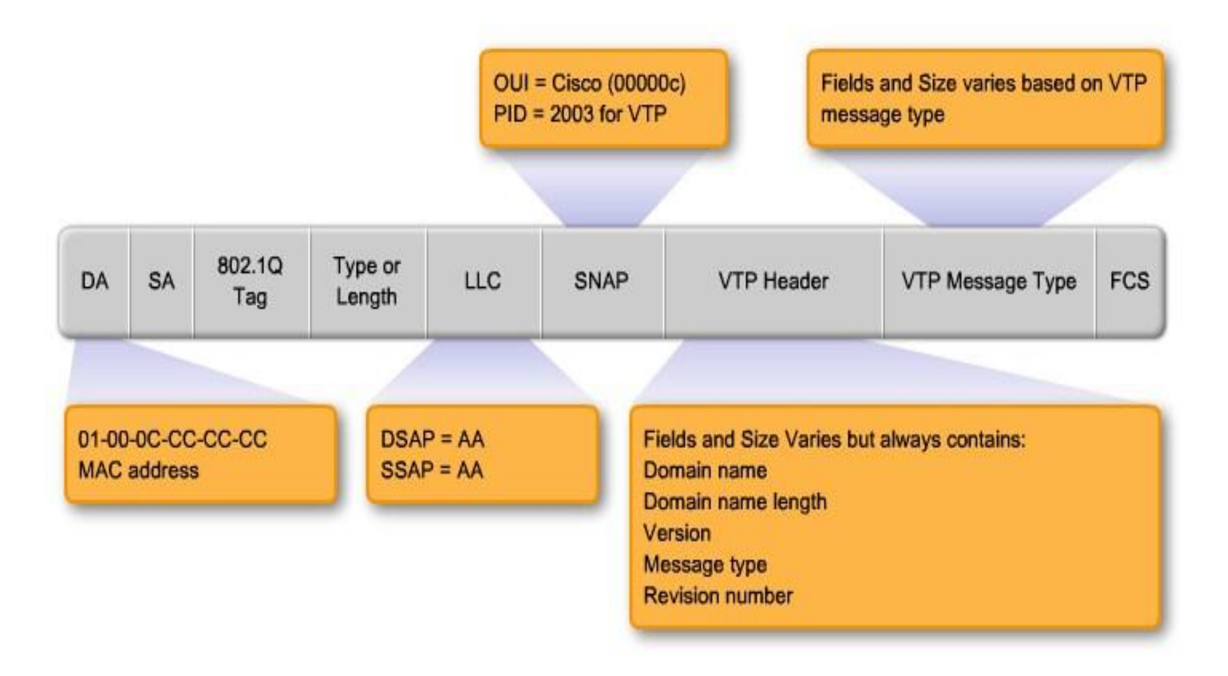
- هذه المكونات التي تكون في داخل رسالة الاعلان والتي تحتوي على التغيرات التي تم تحديثها أو تغيرها و التعديل عليه على مختلف المكونات مثل ما في الصورة .

- **VTP Revision Number :** هذه الخدمة هي عبارة عن قيمة مهم جداً يتم زيدتها في كل مره يتم فيه تعديل البيانات في السويتش .



VTP Frame Structure

هذه عملية بناء الإطار الخاص في بروتوكول الـ VTP



- **VTP Version:** صدارات بروتوكول الـ **VTP** يوجد ثلاث اصدارات :

الإصدار الأول **VTP Version 1** : يدعم شبكات **Token Ring Vlans**.

الإصدار الثاني **VTP Version 2** : يدعم عملية المراقبة

الإصدار الثالث **VTP Version 3** : يدعم ما بين الاصدارين و يعمل بجميع الاعدادات التي تعمل بهم الاصداران الاولى .

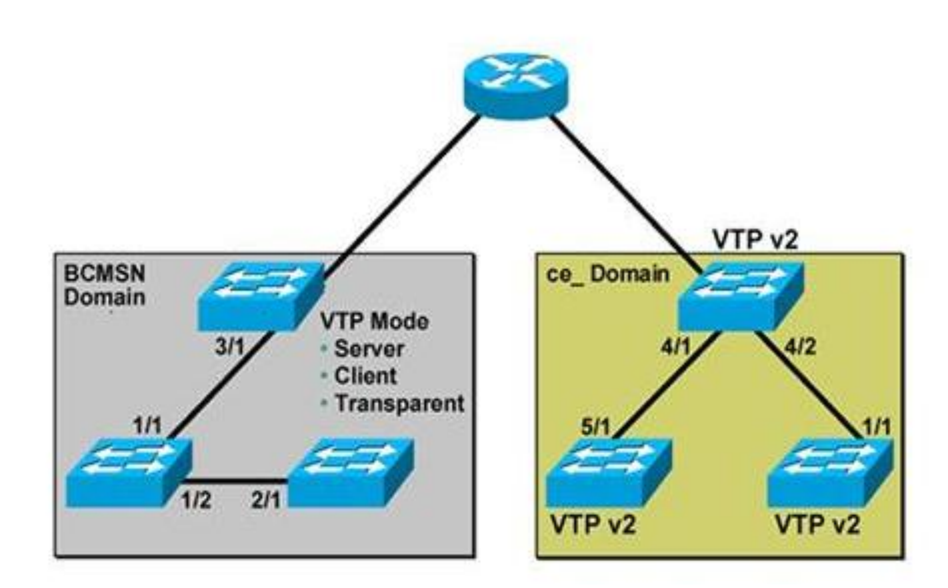
- إعدادات بروتوكول الـ **VTP** المشتركة التي تشترك في جميع السويتشات التي يتم تفعيل بروتوكول الـ **VTP** عليها ، ويجب أن تكون هذه الإعدادات صحيحة في جميع السويتشات ليعمل البروتوكول بشكل صحيح .

1. **VTP Domain Name**
2. **VTP Password**
3. **VTP Version**

Common VTP Configuration Issues

- Incompatible VTP Versions
- VTP Password Issues
- Incorrect VTP Mode Name
- All Switches set to VTP Client Mode

VTP Version



إعدادات بروتوكول الـ VTP
VTP Configuartion



VTP Server

Switch > **enable**

Switch # **config t**

Switch (config) # **vtp domain ABC** ⟵ أسم النطاق

Switch (config) # **vtp version 2**

Switch (config) # **vtp mode server**

Switch (config) # **vtp password 123**

VTP Client

Switch > **enable**

Switch # **config t**

Switch (config) # **vtp domain ABC** ⟵ أسم النطاق

Switch (config) # **vtp version 2**

Switch (config) # **vtp mode client**

Switch (config) # **vtp password 123**

هذه الاوامر التي تستخدم في عرض إعدادات و حالة بروتوكول الـ **VTP** على السويتش.

Switch # **show vtp status**

Switch # **show vtp password**

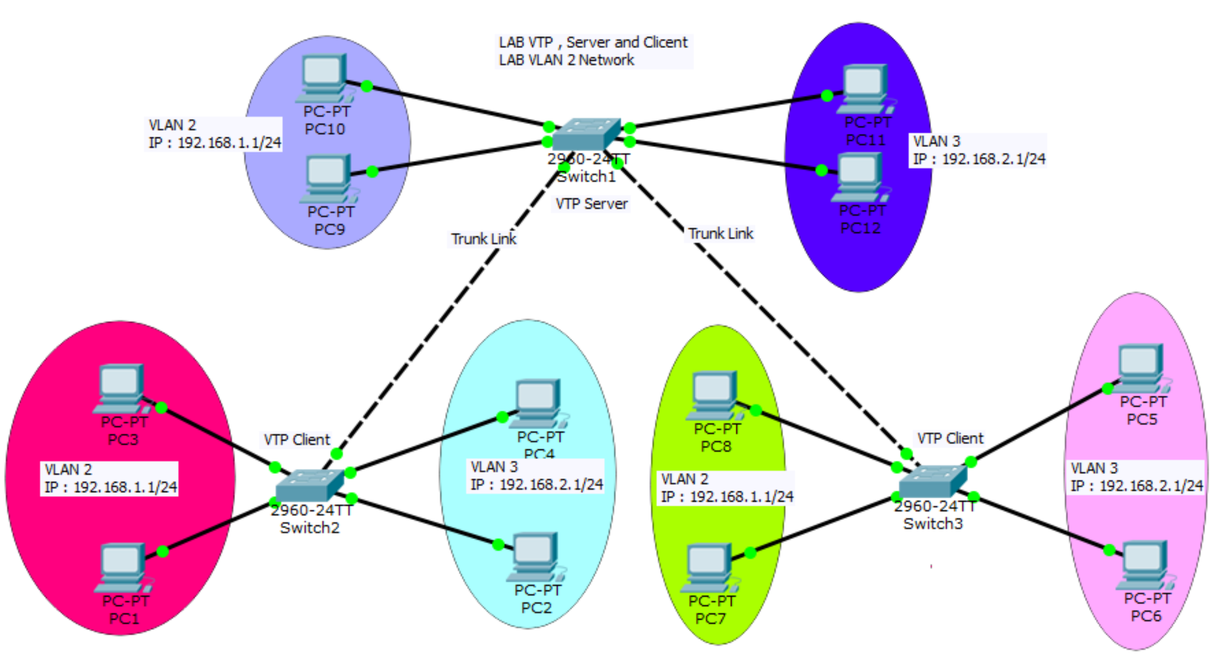
VTP Configuration LAB

إعدادات بروتوكول الـ VTP

- سنقوم بعمل شبكة مكونة من ثلاث سوتيشات و سنقوم بتقسيم شبكات الـ **Vlan** على السويتشات , و سنقوم بتعرف على إعدادات الشبكة :
- في البداية سنقوم بتطبيق عملي على الطوبولوجي المكون من شبكتين **Vlan** مقسمية على جهاز السويتش الأول و هو الـ **VTP Server** و بعده سنقوم بربط باقي السويتشات مع السويتش الرئيسي و سيكون الربط **Trunk Port** ما بين السويتشات ليتم العمل بشكل صحيح .

- **إعدادات الشبكة :**

١. الشبكة الأولى ستكون بعنوان **192.168.1.0/24** هذا عنوان الشبكة الأولى و التي ستاخذ رقم شبكة الـ **Vlan 2** و اسم الشبكة **Name IT** .
٢. الشبكة الثانية ستكون بعنوان **192.168. 2.0/24** هذا عنوان الشبكة الثانية والتي ستاخذ رقم الشبكة **Vlan 3** و اسم الشبكة **Name HR** .
٣. سنقوم بتركيب عنوان الاي بي على كل أجهزة الحاسوب على حسب ترتيب الشبكة المنتمي اليه أجهزة الحاسوب .
٤. سيكون السويتش الرئيسي **SW 1** هذا السويتش الذي سيكون **VTP Server** و تحت هذا السويتش سيكون **SW 2** و **SW 3**، ستكون هذه السويتشات **VTP Client** كما في النموذج التالي .



- الأن بهذا الشكل نكون قد تم الانتهاء من عمل إعدادات الشبكات بشكل كامل و عمل الإعدادات على السويتش الأول و هو الـ **VTP Server** بعد ذالك سنقوم بعمل تفعيل لبروتوكل الـ **VTP** لتتم عملية تبادل المعلومات و الشبكات بشكل صحيح .

- الأن ياتي دور بروتوكول الـ **VTP** أنظر للنموذج يوجد ثلاث سويتشات و نريد أن تكون عليهم شبكة الـ **Vlan** بدل من أن نقوم بدخول على كل سويتش و نقوم بعمل الإعدادات سنقوم فقط بتفعيل بروتوكول الـ **VTP**، على السويتش الرئيسي و نقوم بتفعيله ايضاً على السويتشات التي تحت السويتش الرئيسي ليتم تبادل المعلومات و الشبكات تابع الإعدادات .

- الأن سنقوم بدخول على الـ **SW 1** و عمل الإعدادات التالية :

الأن سنقوم بكتابة الاوامر التالية :

Switch > **enable**

Switch # **config t**

Switch (config) # **vtp domain ABC** ⟵ أسم النطاق

Switch (config) # **vtp version 2**

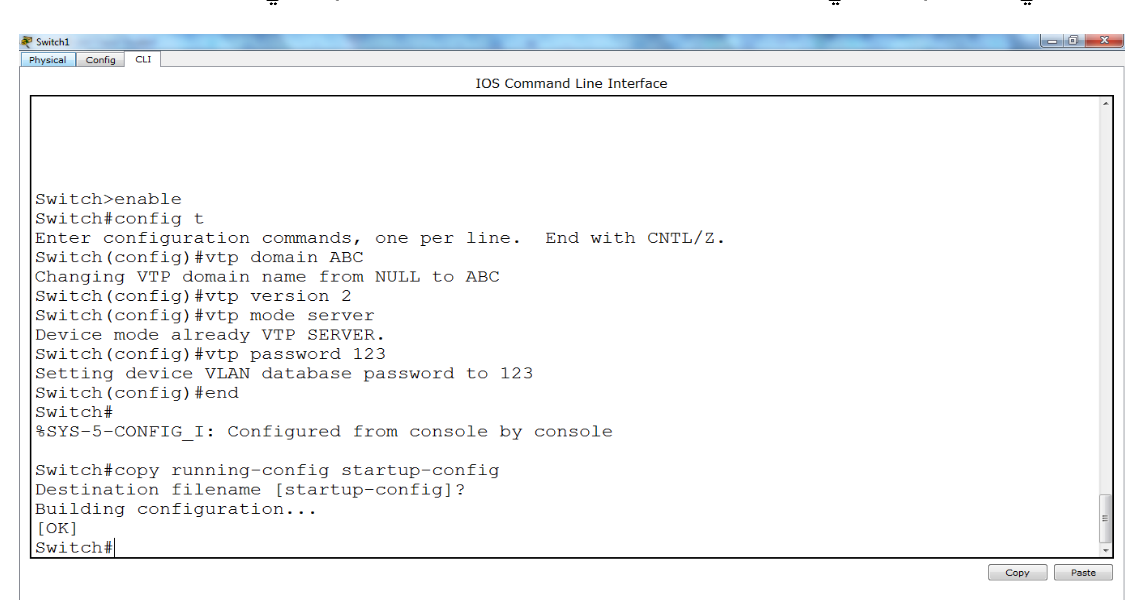
Switch (config) # **vtp mode server**

Switch (config) # **vtp password 123**

Switch (config) # **end**

Switch # **copy running-config startup-config**

كما في الصورة التالي من داخل **SW 1** و هو السويتش الرئيسي **VTP Server**

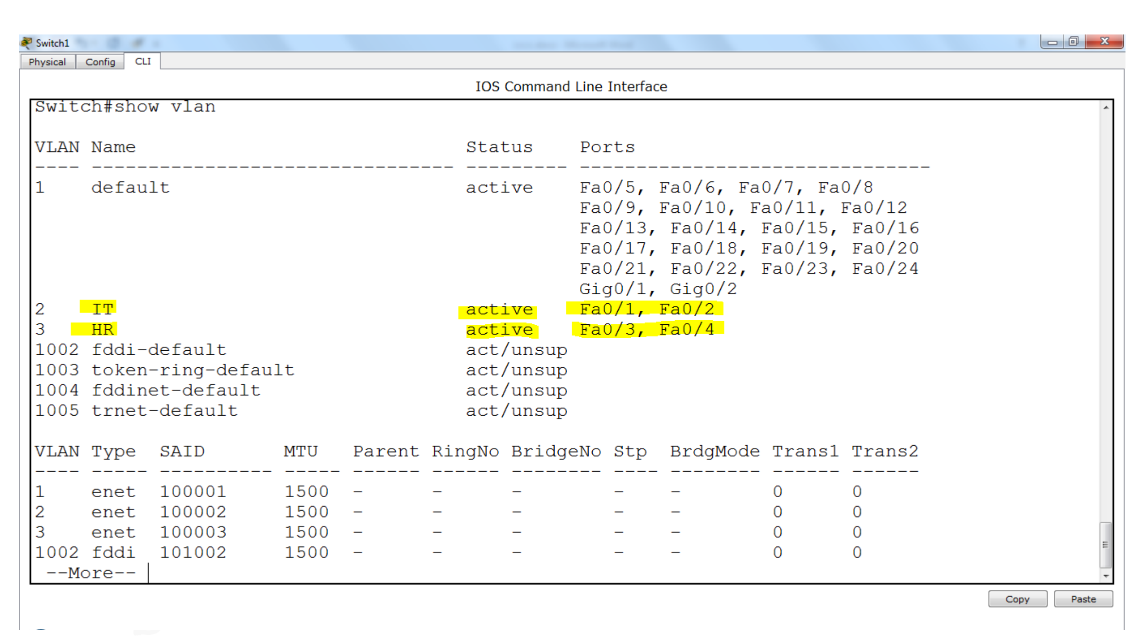


ملاحظة مهم جداً جداً : نحن قمنا بإنشاء شبكات الـ **Vlan** من قبل على السويتش الأول **SW 1** فقط ، اما الأن نحن لقد قمنا بتفعيل بروتوكول الـ **vtp** ليتم تبادل المعلومات و الشبكات على السويتشات الآخر التي تحت نطاق الـ **VTP Server** .

- قبل أن نقوم بتفعيل بروتوكول الـ **vtp** على باقي السويتشات سنقوم بدخول على **SW 1** و نستعرض شبكات الـ **Vlan** و نستعرض إعدادات الـ **vtp** لنكون على دراية كاملة ماذا حدث قبل أن نقوم بدخول على السويتشات الآخر نتابع .

- أنظر للصورة التالية إنه من داخل **SW 1** لاحظ إنه يوجد شبكات **Vlan** باسم **HR , IT** هذا يعني إنه يوجد شبكات على السويتش .

SW 1



```
Switch#show vlan

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                                Gig0/1, Gig0/2
2    IT                               active    Fa0/1, Fa0/2
3    HR                               active    Fa0/3, Fa0/4
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
1    enet  100001     1500  -      -      -        -    -        0      0
2    enet  100002     1500  -      -      -        -    -        0      0
3    enet  100003     1500  -      -      -        -    -        0      0
1002 fddi  101002     1500  -      -      -        -    -        0      0
 --More--
```

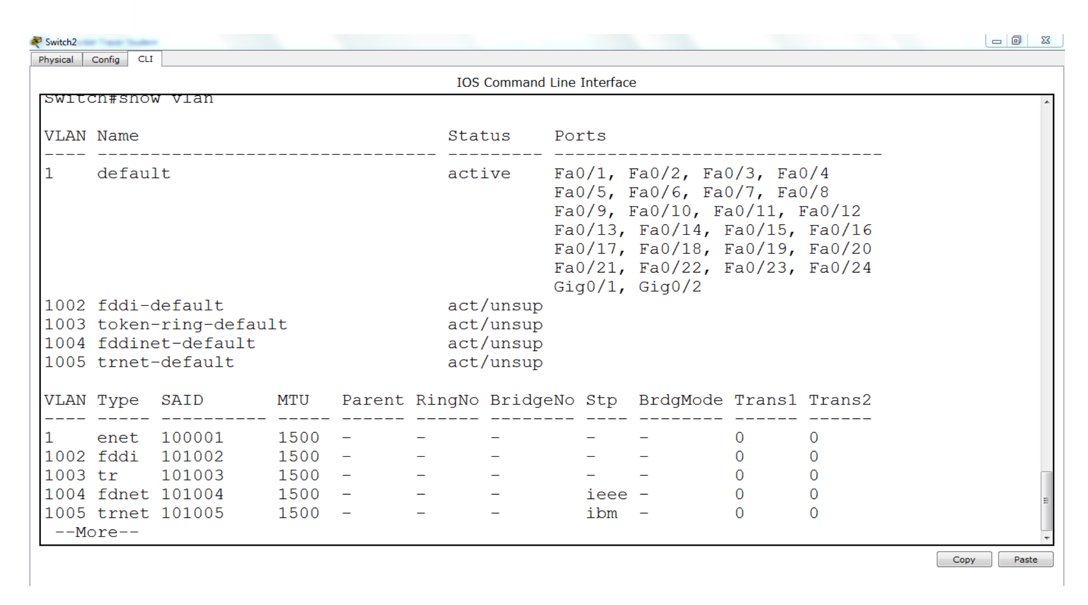
- إعدادات الـ **vtp** ايضاً على **SW 1** أنظر عليها في الصورة التالي لنتاكد من إنه هذا هو السويتش الرئيسي **VTP Server**.

```
Switch#show vtp status
VTP Version                     : 2
Configuration Revision          : 1
Maximum VLANs supported locally : 255
Number of existing VLANs        : 7
VTP Operating Mode              : Server
VTP Domain Name                 : ABC
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Enabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0x85 0x47 0xDE 0xC7 0x79 0x83 0x86 0x00
Configuration last modified by 0.0.0.0 at 3-1-93 00:43:33
Local updater ID is 0.0.0.0 (no valid interface found)
```

- بهذا الشكل تكون جميع الإعدادات صحيحه ويبقى علينا أن نقوم بدخول على السويتشات الآخر لنتاكد هل الشبكات تم نقلها أو لا ويجب أن نعلم أنه لا يمكن نقله , الا إذا قمنا بتفعيل بروتوكول الـ **VTP** عليهم ليتم تبادل المعلومات و الشبكات تابع .

- أنظر للصورة التالي من داخل الـ **SW 2** لا يوجد اي شبكة هذا يدل على إنه لم يتم تفعيل بروتوكول الـ **VTP** على السويتش **SW 2** .

SW 2



- الأن سنقوم بدخول على الـ **SW 2** و عمل الإعدادات التالية :

الأن سنقوم بكتابة الاوامر التالية :

Switch > **enable**

Switch # **config t**

Switch (config) # **vtp domain ABC** ⟵ أسم النطاق

Switch (config) # **vtp version 2**

Switch (config) # **vtp mode client**

Switch (config) # **vtp password 123**

Switch (config) # **end**

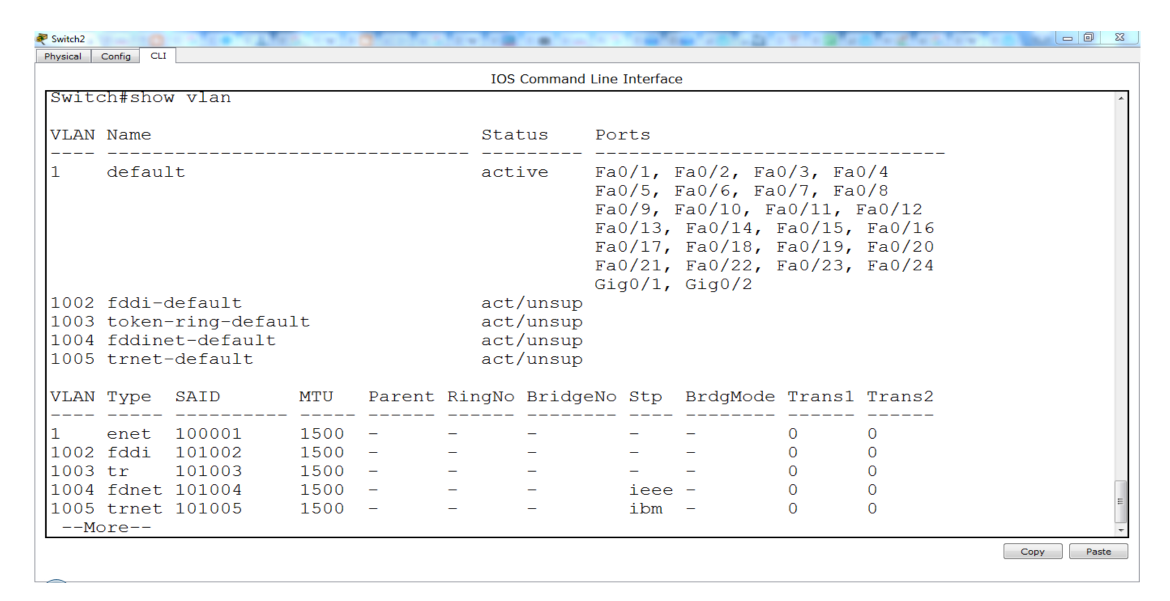
Switch # **copy running-config startup-config**

```
Switch>enable
Switch#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#vtp domain ABC
Changing VTP domain name from NULL to ABC
Switch(config)#vtp version 2
Switch(config)#vtp mode client
Setting device to VTP CLIENT mode.
Switch(config)#vtp password 123
Setting device VLAN database password to 123
Switch(config)#end
Switch#
%SYS-5-CONFIG_I: Configured from console by console

Switch#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
```

- الأن سنقوم ايضاً بدخول على الـ **SW 2** و نقوم بعرض شبكات الـ **Vlan** لنرى هل تم اضافته و تبادل المعلومات من السويتش الرئيسي أو لا .

SW 2



```
Switch#show vlan

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                                Gig0/1, Gig0/2
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
1    enet  100001     1500  -      -      -        -    -        0      0
1002 fddi  101002     1500  -      -      -        -    -        0      0
1003 tr    101003     1500  -      -      -        -    -        0      0
1004 fdnet 101004     1500  -      -      -        ieee -        0      0
1005 trnet 101005     1500  -      -      -        ibm  -        0      0
 --More--
```

- لاحظ إنه لا يوجد ولا شبكة **Vlan** و مع العلم لقد قمنا بتفعيل بروتوكول الـ **vtp** على السويتش **SW 2** , ولكن لم نقم بعمل إعدادات المنفذ الذي يربط ما بين السويتش الأول **SW 1** و السويتش الثاني **SW 2** , يجب أن نقوم بعمل الإعدادات على المنفذ ليكون **Trunk Port** ليستطيع إرسال البيانات من سويتش الى اخرى , سنقوم بدخول على السويتش الأول **SW 1** و نقوم بعمل إعدادات المنفذ الذي يربط ما بين السويتشات تابع التالي .

- سنقوم بدخول على السويتش الأول **SW 1** و نقوم بعمل الإعدادات الخاصة في المنفذ الذي سيكون **Trunk Port** :

```
Switch>enable
Switch#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#interface fastethernet 0/1
Switch(config-if)#switchport mode trunk

Switch(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up

Switch(config-if)#exit
Switch(config)#interface fastethernet 0/2
Switch(config-if)#switchport mode trunk

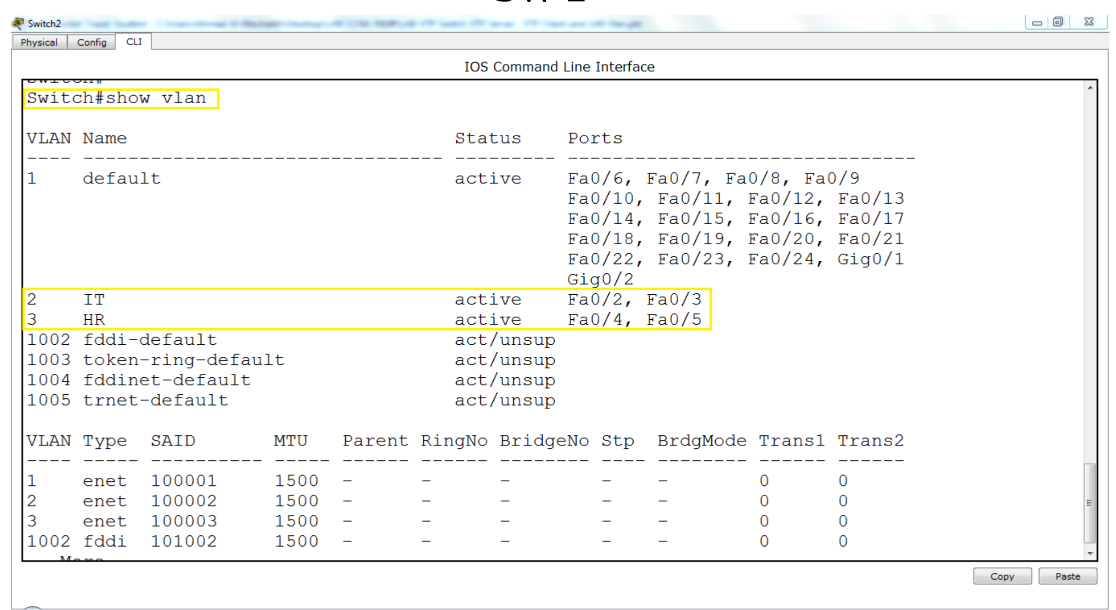
Switch(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to up
```

- لاحظ في هذه الصورة من داخل **SW 1** قمنا بعمل إعدادات منفذ الـ**Trunk Port** على منفذين **f0/1 , f0/2** المنفذ الأول المتصل في الـ **SW 2** و المنفذ الثاني المتصل في **SW 3** الأن بهذا الشكل نكون قد قمنا بعمل الإعدادات الخاص في المنافذ .

- الأن سنقوم بدخول على السويتش الثاني **SW 2** و نتاكد هل تم تبادل الشبكات و المعلومات أو لا أنظر للصورة التالية من داخل السويتش الثاني :

SW 2



```
Switch#show vlan

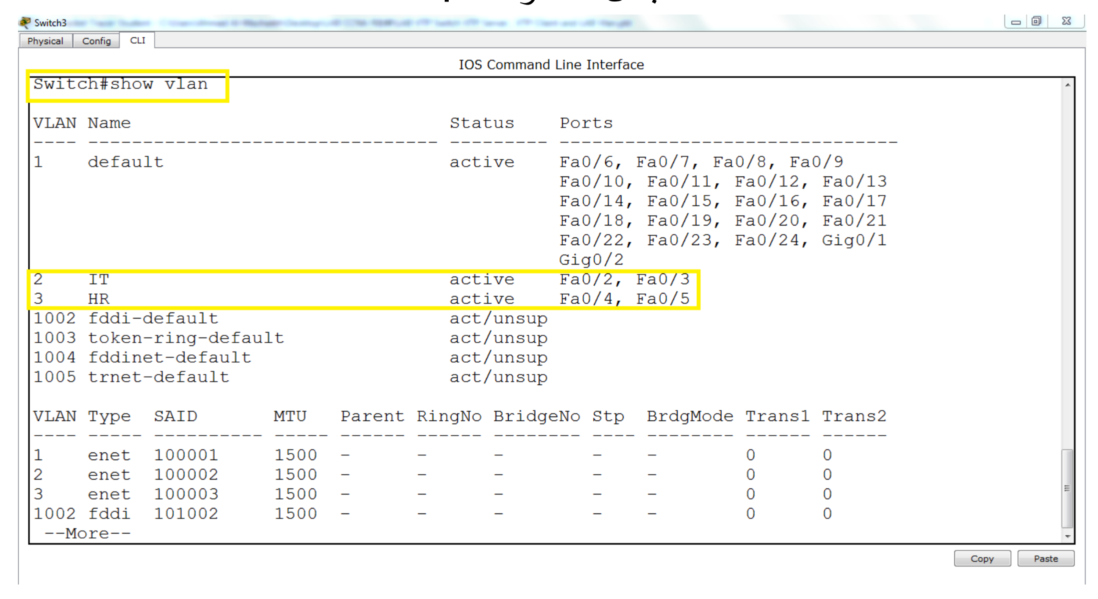
VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/6, Fa0/7, Fa0/8, Fa0/9
                                                Fa0/10, Fa0/11, Fa0/12, Fa0/13
                                                Fa0/14, Fa0/15, Fa0/16, Fa0/17
                                                Fa0/18, Fa0/19, Fa0/20, Fa0/21
                                                Fa0/22, Fa0/23, Fa0/24, Gig0/1
                                                Gig0/2
2    IT                               active    Fa0/2, Fa0/3
3    HR                               active    Fa0/4, Fa0/5
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
1    enet  100001     1500  -      -      -        -    -        0      0
2    enet  100002     1500  -      -      -        -    -        0      0
3    enet  100003     1500  -      -      -        -    -        0      0
1002 fddi  101002     1500  -      -      -        -    -        0      0
```

- لاحظ إنه تم وجد الشبكات و تم تبادل المعلومات بشكل صحيح الأن سنذهب للسويتش الثالث لنرى هل تم تبادل المعلومات و الشبكات أو لا .

- الأن سنقوم بدخول على السويتش الثالث ولكن الان اقوم بشرح الإعدادات نفسها فقط سأقوم بعرض الشبكات و نتاكد هل تم اضافته أو لا .

أنظر للصورة التالية من داخل السويتش الثالث **SW 3** و لاحظ إنه تم إضافة الشبكات و تبادل المعلومات :



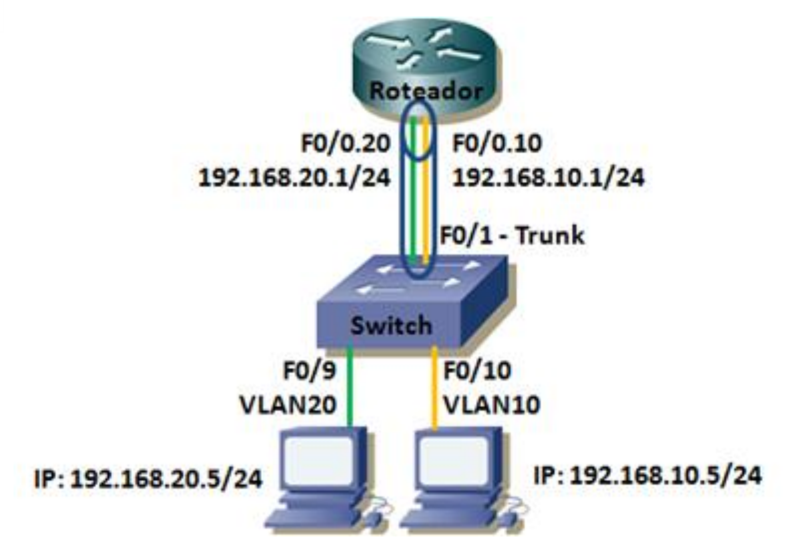
```
Switch#show vlan

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/6, Fa0/7, Fa0/8, Fa0/9
                                                Fa0/10, Fa0/11, Fa0/12, Fa0/13
                                                Fa0/14, Fa0/15, Fa0/16, Fa0/17
                                                Fa0/18, Fa0/19, Fa0/20, Fa0/21
                                                Fa0/22, Fa0/23, Fa0/24, Gig0/1
                                                Gig0/2
2    IT                               active    Fa0/2, Fa0/3
3    HR                               active    Fa0/4, Fa0/5
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
1    enet  100001     1500  -      -      -        -    -        0      0
2    enet  100002     1500  -      -      -        -    -        0      0
3    enet  100003     1500  -      -      -        -    -        0      0
1002 fddi  101002     1500  -      -      -        -    -        0      0
 --More--
```

- بهذا الشكل يكون قد تم الانتهاء من درس بروتوكول الـ **VTP** .

Router on a Staick



- **Router on a Staick:** هذه الخدمة مهم جداً جداً تستخدم عندما يكون لدينا اكثر من شبكة **Vlan** على سويتش واحد و نريد هذه الشبكة أن تتصل مع بعضها البعض و هي على مختلف شبكة الـ **Vlan** و على سويتش واحد، فهذه الخدمة تقوم بهذه الوظيفة و تقوم بربط شبكة الـ **Vlan** المختلفة مع بعضها البعض و أن يتصلوا مع بعض عن طريق منفذ واحد و هو منفذ الراوتر نقوم بتقسيمها لعدة اقسام بشكل وهمي و نقوم بتوزيع الـ **Gy** على حسب تقسيم المنفذ لكل شبكة.

- **مثال على الـ Router on a Staick** : لنفترض إنه لدينا اربعة شبكات **Vlan** بمختلف العناوين على سويتش واحد ، و نريد من هذه الشبكات أن تتصل مع بعضها البعض من الطبيعي جداً أن نحتاج لجهاز راوتر ليربط ما بين هذه الشبكات سنقوم بتركيب جهاز الراوتر و تقسيم الإنترفيس الواحد الى عدة انترفيس و نقوم بتوزيعهم على شبكات الـ **Vlan** و نقوم بضبط الإعدادات الخاص في الـ **Router on a Staick** ليتم العمل بشكل صحيح .

- سنقوم بعمل الإعدادات على المنوذج التالية لاحظ إنه يوجد اربع شبكات **Vlan** مختلفة العناوين و نريد أن تتصل مع بعضها البعض عن طريق الراوتر و لاحظ ايضاً إنه تم ربط منفذ واحد من الراوتر الى السويتش هذا يدل على إنه يوجد انترفيس اوحد متصل في السويتش هذا صحيح ، و نحن سنقوم بتقسيم هذا الإنترفيس الى عدة انترفيس على حسب عدد الشبكات الموجودة لدينا و تركيب الـ **Gy** على كل شبكة و توزيعها على الشبكات لتستطيع جميع الشبكات الاتصال مع بعضها البعض ، كل هذه العملية على سويتش واحد و راوتر واحد سنقوم بعمل الإعدادات التالية قبل أن نقوم بدخول على الراوتر و نقوم بتفعيل خدمة الـ **Router on a Staick** تابع الإعدادات التالية .

Router on a Staick Configuration

إعدادات الـ Router on a Staick



Router > **enable**

Router # **config t**

Router (config) # **interface fastethernet 0/0**

Router (config-if) # **no shutdown**

Router (config-if) # **exit**

Router (config) # **interface fastethernet 0/0.1** ⟵ subif

Router (config-subif) # **encapsulation dot1Q 2** ⟵ رقم الشبكة

Router (config-subif) # **ip address 192.168.1.100 255.255.255.0**

- أنظر للمنوذج التالي هذا هو الذي سنقوم بتطبيق عليه خدمة الـ Router on a Staick ، و لاحظ ايضاً إنه يوجد اربعة شبكات **VLAN** بمختلف العناوين ونحن نريد هذه الشبكات أن تتصل مع بعضها البعض سنقوم بتفعيل خدمة الـ Router on a Staick على جهاز الراوتر .

LAB Router on a Stick and Vlan 4 Network and Protocol Trunk dotQ1 and sub interface

2811
Router1

PC-PT PC6
PC-PT PC5
Vlan 4 Name PR
IP Address 192.168.3.0/24

PC-PT PC8
PC-PT PC7
Vlan 5 Name AC
IP Address 192.168.4.0/24

2960-24TT
Switch1

PC-PT PC1
PC-PT PC2
Vlan 2 Name IT
IP Address 192.168.1.0/24

PC-PT PC3
PC-PT PC4
Vlan 3 Name HR
IP Address 192.168.2.0/24

- **ملاحظة مهم جداً** : يجب أن نعرف أن المنفذ المتصل من السويتش الى الراوتر سيكون ايضاً منفذ **Trunk Port** ليستطيع الإرسال و الاستقبال .

- الأن سنقوم بدخول على جهاز الراوتر **R1** و نقوم بعمل الإعدادات التالية :

الأن سنقوم بكتابة الاوامر التالية :

```
Router > enable
Router # config t
Router (config) # interface fastethernet 0/0
Router (config-if) # no shutdown
Router (config-if) # exit
Router (config) # interface fastethernet 0/0.1
 Router (config-subif) # encapsulation dot1q 2
Router (config-subif) # ip address 192.168.1.100 255.255.255.0
Router (config-subif) # exit
Router (config) # interface fastethernet 0/0.2
 Router (config-subif) # encapsulation dot1q 3
Router (config-subif) # ip address 192.168.2.100 255.255.255.0
Router (config-subif) # exit
Router (config) # interface fastethernet 0/0.3
 Router (config-subif) # encapsulation dot1q 4
Router (config-subif) # ip address 192.168.3.100 255.255.255.0
Router (config-subif) # exit
Router (config) # interface fastethernet 0/0.4
 Router (config-subif) # encapsulation dot1q 5
Router (config-subif) # ip address 192.168.4.100 255.255.255.0
Router (config-subif) # end
Router # copy running-config  startup-config
```

- هذه إعدادات الإنترفيس **f0/0** الخاصة في جهاز الراوتر و قمنا ايضاً بتفعيل خدمة الـ **Router on a Staick**، و الأن يتبقى علينا عمل الإنترفيس المتصل من السويتش الى الراوتر لجعله **Trunk Port** ليتسطيع الاتصال في الشبكات و نقل البيانات ما بينهم تابع ...
- سنقوم بدخول على جهاز السويتش و نقوم بعمل إعدادات المنفذ المتصل من السويتش الى الراوتر و سيكون المنفذ **f0/24** المتصل في جهاز الراوتر سنقوم بعمل الإعدادات التالية :

Switch > **enable**
Switch # **config t**
Switch (config) # **interface fastethernet 0/24**
Switch (config-if) # **switchport mode trunk**

- بهذا الشكل نكون قد قمنا بعمل جميع الإعدادات الخاصة في خدمة الـ **Router on a Staick** ، و سنقوم بتركيب الـ **Gy** الخاص في كل شبكة على كل أجهزة الحاسوب التي تحت كل شبكة من شبكة الـ **Vlan** .

- الأن نريد التاكد من جميع الإعدادات التي قمنا بعملها تم تنفيذها أو لا عن طريق الدخول على جهاز الراوتر و نقوم بعرض الإنترفيس و نرى ماذا حدث تابع ....

- سنقوم بكتابة الأمر التالي ليقوم بعرض معلومات عن الإنترفيس بشكل مرتب .....

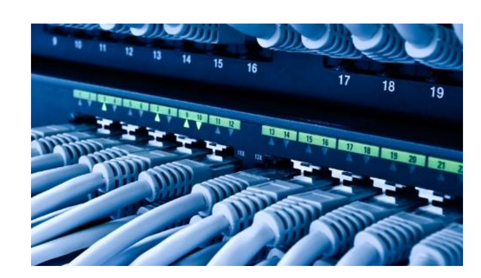
Router # **Show ip interface brief**

```
R1#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
FastEthernet0/0        unassigned      YES unset  up                    up
FastEthernet0/0.1      192.168.1.100   YES manual up                    up
FastEthernet0/0.2      192.168.2.100   YES manual up                    up
FastEthernet0/0.3      192.168.3.100   YES manual up                    up
FastEthernet0/0.4      192.168.4.100   YES manual up                    up
FastEthernet0/1        unassigned      YES unset  administratively down down
Vlan1                  unassigned      YES unset  administratively down down
R1#
```

- لاحظ إنه يوجد اربع منافذ كل منفذ ياخذ عنوان اي بي مختلف عن الآخر و المنفذ الرئيسي **f0/0** لا يحتوي على عنوان اي بي هو فقط مفعل اما الإنترفيس الذي تخضع تحت هذا الإنترفيس هي منافذ وهمية و ياخذ كل منفذ عنوان ينتمي لشبكة **Vlan** .
- **توضيح بسيط** : عندما يريد جهاز معين في شبكة **Vlan 1** يريد الاتصال في جهاز موجود في شبكة **Vlan 2** سيتم الاتصال عن طريق خدمة الـ **Router on a Staick** .
- بهذا الشكل نكون قد اكملنا كامل الدرس الخاص في خدمة الـ **Router on a Staick** بشكل كامل .

حالات منافذ السوتيش

Switch Port Modes



- حالات منافذ السوتيش تبداء عندما نقوم بتوصيل جهاز حاسوب أو سوتيش أو راوتر أو ما شابه في منفذ السويتش , حيث يقوم منفذ السوتيش باخذ بعض الوقت ليقوم بتحديد حالة المنفذ , و يوجد اكثر من حالة لتحديد المنفذ سأقوم بذكرهم .

1- Dynamic Desirable
2- Trunk
3- Access
4- Dynamic Auto Access
5- No Negotiate
6- DTP = Dynamic Trunking Protocol

Dynamic Desirable : هذه الحالة تعتمد على نوع التوصيل التلقائي مثل عندما نقوم بعمل منفذ **Trunk Port** على أحد السويتش , و قمنا بتوصيل الكابل الذي يخرج من هذا المنفذ بربطه في سوتيش اخرى سيقوم المنفذ الذي على السويتش الآخر ياخذ حالة المنفذ المقابل لديها بشكل تلقائي من غير تدخل من مهندس الشبكة .

مثال على Dynamic Desirable : لو قمنا بربط سوتشين مع بعضهم البعض و كان حالة منفذ السويتش الذي يتصل في السويتش الآخر **Access** سيتم بشكل تلقائي المنفذ الذي في السويتش الآخر ياخذ حالة الـ **Access** هذه وظيفة الـ **Dynamic Desirable**.

Trunk : هذه حالة المنافذ التي ستكون **Trunk Port** و التي تعمل على الربط ما بين السويتشات و الراوترات لتبادل المعلومات ما بينهم.

Access : هذه حالة المنافذ التي ستكون **Access** و التي تعمل على ربط جهاز حاسوب مع سويتش.

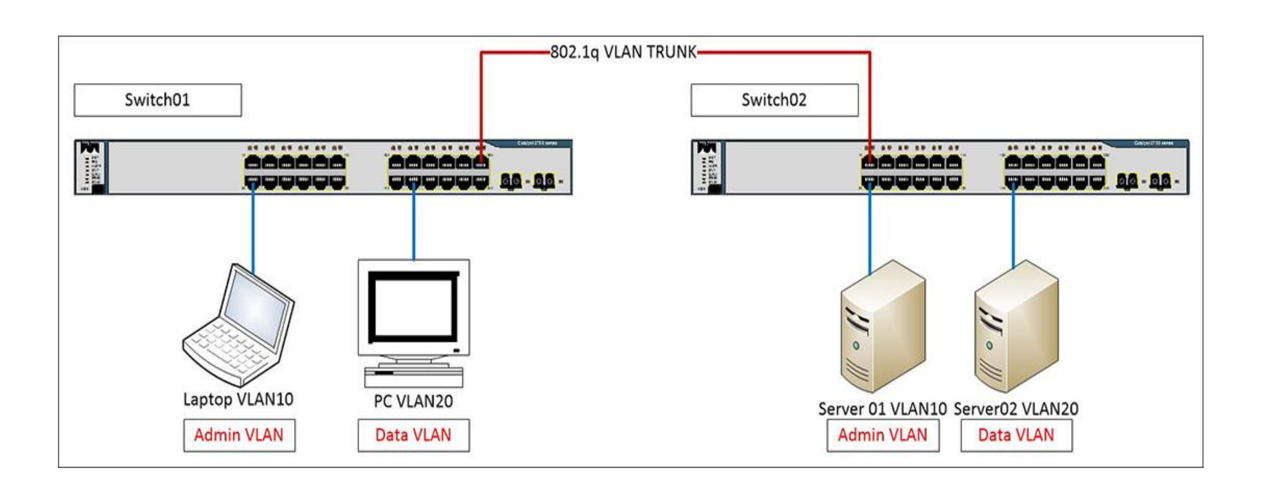
Dynamic Auto Access : هذه حالة المنفذ الذي سيتم تحديده بشكل اتوماتيكي مثل عندما يتم تحويل المنفذ لـ **Access** سيتم تحويل المنفذ المتصل فيه الـ **Access** أو إذا كان **Trunk** سيتم تحويل المنفذ المقابل له **Trunk**.

No Negotiate : هذه حالة المنافذ التي تمنع عملية التفاوض بمعنى توقيف المنفذ عن الاختيار.

جداول توضيحي لحالة المنافذ

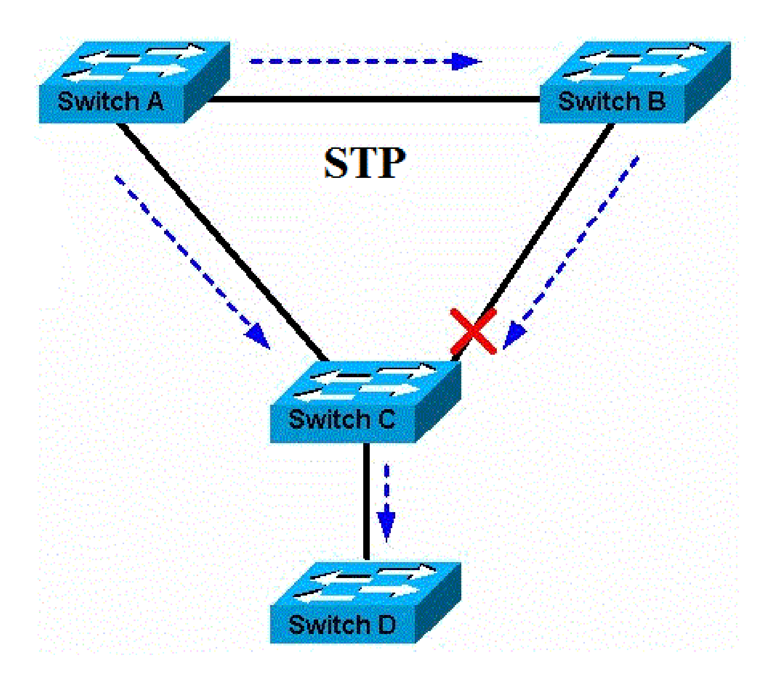
	Dynamic Auto	Dynamic Desirable	Trunk	Access
Dynamic Auto	Access	Trunk	Trunk	Access
Dynamic Desirable	Trunk	Trunk	Trunk	Access
Trunk	Trunk	Trunk	Trunk	?
Access	Access	Access	?	Access

Administrative Mode	Access	Dynamic Auto	Trunk	Dynamic Desirable
access	Access	Access	Do Not Use[1]	Access
dynamic auto	Access	Access	Trunk	Trunk
trunk	Do Not Use[1]	Trunk	Trunk	Trunk
dynamic desirable	Access	Trunk	Trunk	Trunk



STP

Spanning Tree Protocol



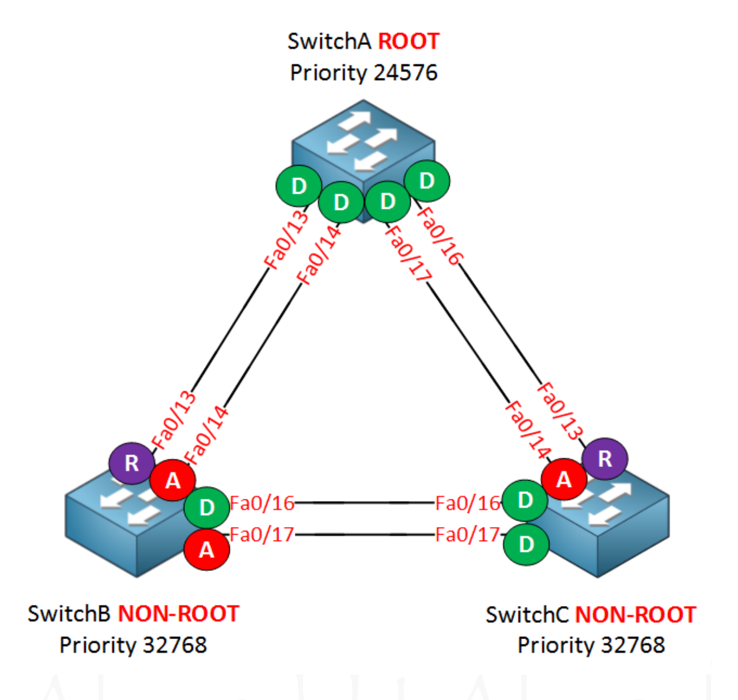
STP: هو عبارة عن بروتوكول وظيفته منع دوران البيانات في السويتشات، فهو يفهمقاعدة تقول إذا تم الربط ما بين سوتشين بلينك واحد لان يحدث دوران للبيانات ولكن إذا تم ربط اكثر من لينك مثل ربط ثلاث أو اربع لينك في هذه الحالة سيحدث عملية دوران البيانات في السويتشات، و هنا تاتي وظيفة بروتوكول الـ **STP** ليقوم بتنظيم الينك و منع دوران البيانات في السويتشات و هذا البروتوكول يعمل بشكل تلقائي من دون أن نقوم بتفعيله على السويتش و يبداء في عملية تنظيم الينك الموجود ، سيقوم باختير لينك واحد لعملية إرسال البيانات و باقي الينكات سيتم ايقافها بشكل مؤقت و في حال حدث عطل ما في الينك الذي يرسل البيانات في هذه الحالة سيقوم بروتوكول الـ **STP** بشكل تلقائي بتشغيل لينك ثاني ليقوم باخذ دور الينك الأولى و يبداء بعملية الإرسال و الاستقال .

- يعمل هذا البروتوكول على مستوى الطبقة الثانية **Data Link Layer**.
- بروتوكول **STP** يعمل على جميع أجهزة السويتش مثل سويتشات سيسكو و **juniper** و هواوي.
- بروتوكول الـ **STP** ينتمي لمنظمة **IEEE** و تصنيفها **802.1D** .

- الأن لنتعرف على عملية اختيار الينك الرئيسي الذي سيتم الاعتماد عليه في نقل المعلومات و الداتا , و باقي الينكات سيتم توقيفها بشكل مؤقت و هذه العملية تتم على عدة خطوات سأقوم بذكر هذه الخطوات و شرحها , ولكن يجب أن نعلم ايضاً إنه يتم انتخاب سويتش رائيسي واحد من مجموعة سويتشات و باقي السويتشات ستكون بشكل احتياطي أو مساعدة للسويتش الرئيسي , ولتتم عملية الانتخاب ايضاً يقوم بعدة خطوات و سأقوم بذكرهم و شرحها ايضاً بالتفصيل الممل .

- مصطلحات السويتشات في بروتوكول الـ STP :

١- السويتش الرائيسي Root Bridge .
٢- السويتش الاحتياطي Non Bridge .



- عملية انتخاب السويتشات و تحديد السويتش الرئيسي **Root Bridge** و السويتش الاحتياطي **Non Bridge** , ولتتم هذه العملية ستمر السويتشات في عدة مراحل سأقوم بذكر هذه المراحل .

- مرحلة عملية الانتخاب تتكون من إرسال رسالة ترحيب **BPDU = Bridge Protocol Data Units** هذه عبارة عن رسالة يتم تبادلها ما بين السويتشات ليتم التعرف على السويتشات و حالتهم , و هل هم موجودين في داخل الشبكة و قيد التشغيل أو لا , بمعنى إنها هذه الرسالة التي تقوم بمعرفة المعلومات الخاصة في جميع السويتشات الموجودة على الشبكة و تتبادلها مع بعضها البعض لتتم عملية الانتخاب .
- محتويات رسالة الـ **BPDU** :

تنقسم رسالة الـ **BPDU** الى عدة اقسام مهمة جداً جداً و يتم الاعتماد عليهم في عملية انتخاب السويتش الرائيسي **Root Bridge** سأقوم بذكر الاقسام .

Bridge ID: هو عبارة عن قيمة رقمية من خلاله يتم اختيار من هو السويتش الذي سيكون **Root Bridge** و من هو السويتش الذي سيكون **Non Bridge** و ينقسم هذا المحتوى الـ **Bridge ID** الى قسمين ..

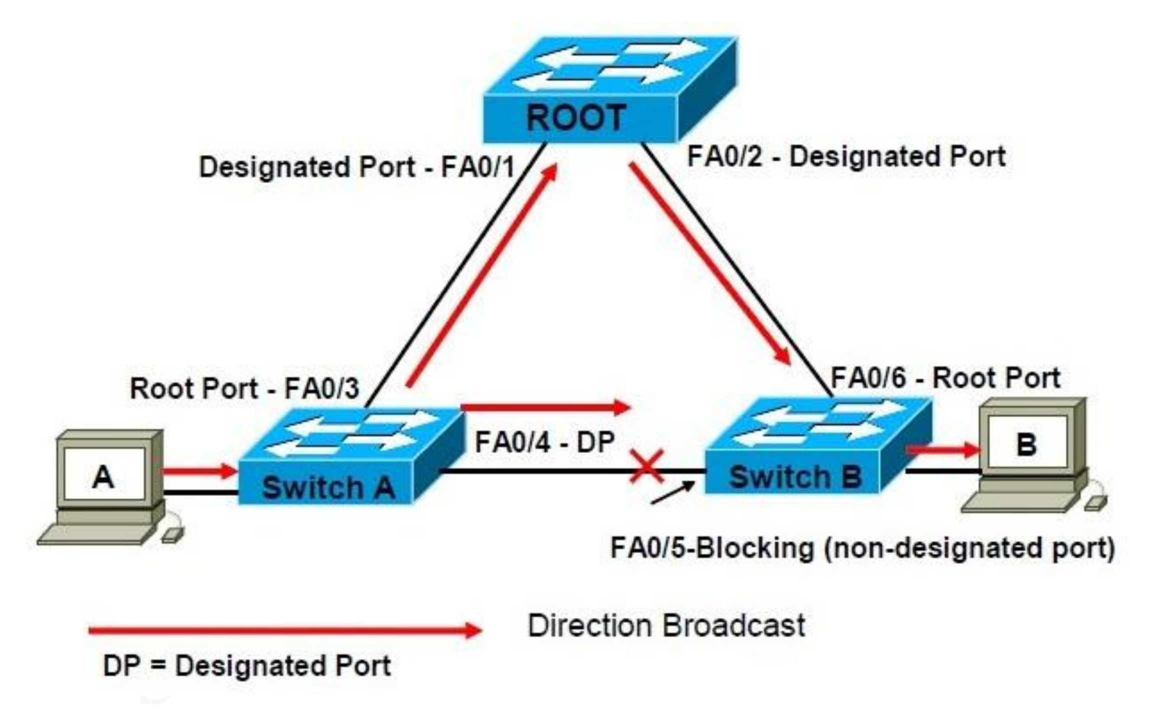
1- Bridge Prioirty , 2- MAC Address

هذه محتويات الى **Bridge ID** سأقوم بشرحها تابع ....

Bridge Prioirty : هي عبارة عن قيمة رقمية للقيمة الأولية الخاصة في جهاز السويتش و تبداء من **0 to 65535** , القيمة الطبيعية تكون **Default Value = 32768**.

Mac Address : هو عبارة عن العنوان الفيزيائي الخاص في جهاز السويتش ولا يتكرر على جهاز اخر .

- **كيف تتم عملية انتخاب السويتش الرائيسي Root Bridge :**



تتم عملية الانتخاب من خلال عدة خطوات تمر فيها رسالة الرتحيب الـ **BPDU** و هي كما شرحنا سابقاً تحتوي على **Bridge Prioirty** و **MAC Address** و سيتم الاعتماد في عملية الانتخاب على هذه المحتويات , في البداية سيتم استكشاف قيمة الـ **Prioirty** في جميع السويتشات و في حال كان قيمة الـ **Prioirty** قليل في أحد السويتشات سيتم انتخابه ليكون السويتش الرئيسي **Root Bridge** , ولكن إذا كانت قيمة الـ **Prioirty** متساوية في جميع السويتشات سيتم تجاوز هذه القيمة و الانتقال الى الـ **Mac Address** ستقوم رسالة الـ **BPDU** بستكشاف العنوان الفيزيائي في جميع السويتشات وكما قلنا سابقاً لكل سويتش عنوان ماك ادرس مختلف لا يتكرر على السويتشات الآخر في هذه الحالة سيتم الاعتماد على اقل عنوان ماك ادرس يمتلكه السويتش ليكون هو السويتش الرئيسي **Root Bridge** و سناخذ بعض الامثلة على هذه الشرح لنستطيع فهم العملية بشكل ممتاز .

- **حالة المنافذ في السويتش مع بروتوكول الـ STP :**

بعد عملية انتخاب السويتش الرائيسي **Root Bridge** و استقرار السويتشات تاتي وظيفة المنافذ التي ستعمل على حسب حالة السويتشات التي تم انتخابها , و في هذه الحالة يوجد ثلاث حالات لمنافذ السويتش التي سيتم اختيارها بشكل مناسب على حسب طبيعية السويتشات التي تعمل في الشبكة سأقوم بذكر الحالة و شرح كل حالة متى تعمل و لماذ تاخذ هذه الحالة.

STP Prot Cost Values

- تحديد تكلفة سرعة المسارات لعملية اختيار المسار, و تتم عن طريق الـ **Cost** و يعتمد على سرعة المنافذ التي على السويتش و بعد تحديد المنفذ و سرعة المنفذ عن طريق الـ **Cost** سيتم تحديد نوع الـ **STP Prot** ليتم تحديد حالته , و هذا الجدول يوضح عملية التكلفة لكل السرعات الموجودة .

Link Speed(Bandwidth)	Port Cost
10 mbps	100
100 bmps	19
1 gbps	4
10 gbps	2

إشكال حالة المنافذ STP Port :

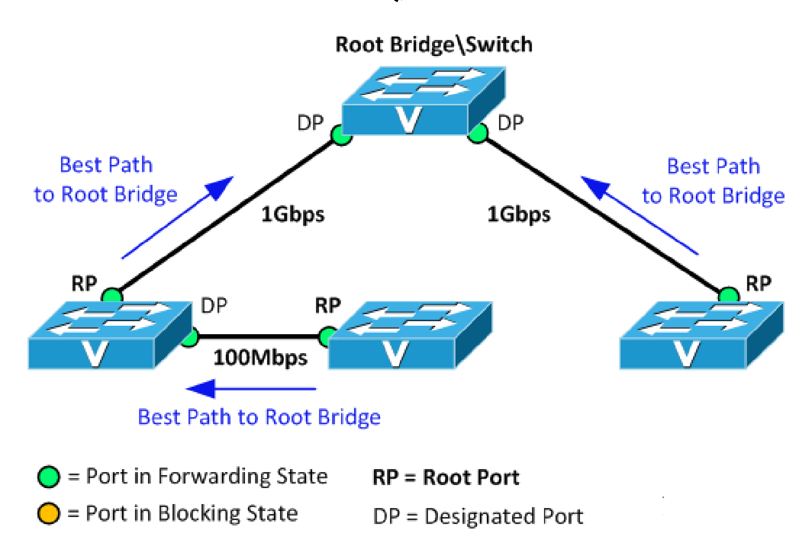
1- **DP = Designated Port**
2- **RP = Root Port**
3- **BP = Block Port**

DP = Designated Port : هذه حالة المنافذ التي تكون على السويتش الرائيسي **Root Bridge** و هي تعمل بشكل طبيعي و تقوم بعملية إرسال و استقبال البيانات.

RP = Root Port : هذا المنفذ ايضاً يعمل على استقبال و إرسال البيانات ولكن هذه الحالة من المنافذ تكون على سويتش الـ **Non Bridg** و تكون متصلة مع السويتش الرائيسي **Root Bridge** و يكون صاحب التكلفة الاقل في المسارات .

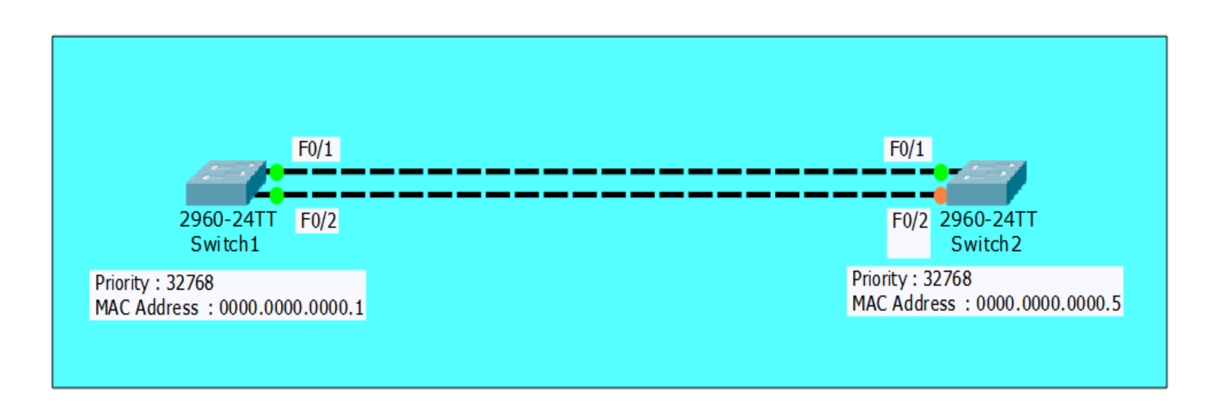
ملاحظة مهم جداً : السويتش الرائيسي تكون حالة المنافذ عليه **DP** ولا تكون **RP** بمعنى أن منافذ الـ **RP** فقط تكون على السويتشات **Non Bridg** فقط .

BP = Block Port : هذا المنفذ المغلق الذي ياخذ اعلى تكلفة **Cost**.



- بهذه الطريقة نكون قد فهمنا كيفية تتم عملية الانتخاب و حالة المنافذ و تكلفة سرعة المسار , الأن سأقوم بعرض بعض الامثلة لنفهم و نحلل كيفية عمل بروتوكول الـ **STP** و سأقوم بعرض اكثر من نموذج لنستيطع فهم بروتوكول الـ **STP** بشكل ممتاز لأنه بروتوكول مهم جداً جداً ويجب أن نكون على معرفة و اتقان و فهم هذا البروتوكول .

- النموذج الأول مكون من سويتشين **SW 1 , SW 2** و نلاحظ إنه تم ربطهم من خلال **2** لينك , ونلاحظ ايضاً إنه تم ايقاف أحد الينكات في هذه الحالة يجب أن نعرف أن بروتوكول الـ **STP** قام بعملية الانتخاب و قام بتحديد لينك واحد لعملية إرسال و استقبال البيانات و تم تحديد سويتش رائيسي **Root Bridge** , بمعنى في هذه الحالة لا يوجد ما يمسى دوران البيانات في الشبكة سنقوم بنظر على النموذج و بعده سأقوم بشرح النموذج بشكل كامل أنظر للنموذج التالي :



- لاحظ في النموذج إنه تم اختيار سويتش رائيسي **Root Bridge** و هذا السويتش هو **SW 1** , الأن لنعرف كيف تمت عملية الانتخاب أنظر للنموذج يظهر فيه السويتشان قيمة الـ **Prioirty 32768** متساوية في الـ **SW 2 , SW 1** في هذه الحالة سيتم تجاوز هذه المرحلة و الانتقال الى المرحلة التالية و هي استكشاف عنوان الماك ادرس للسويتشات أنظر للماك ادرس يوجد اختلاف **SW 1** عنوان الماك ادرس لديه **MAC Address : 0000.0000.0000.1** و عنوان الماك ادرس لـ **SW 2 MAC Address : 0000.0000.0000.2** في هذه الحالة سيتم انتخاب الـ **SW 1** لي لأنه يحتوي على الماك ادرس الاقل كما شرحنا سابقاً و قولنا السويتش الذي يحتوي على ماك ادرس اقل هو الذي سيكون السويتش الرائيسي **Root Bridge** و في هذا النموذج سيكون السويتش الرائيسي هو الـ **SW 1** , سنقوم بدخول على السويتشات و ننظر على المعلومات الموجودة في كل سويتش و نتاكد ايضاً من هو السويتش الرائيسي **Root Bridge** و نتاكد ايضاً من حالة المنافذ .

الأن سنقوم بدخول على السويتش الأول **SW 1** و نقوم باستعرض المعلومات الخاصة في بروتوكول الـ **STP** :

الأن سنقوم بكتابة الاوامر التالية :

Switch > **enable**

Switch # **show spanning-tree**

SW 1

Interface	Role	Sts	Cost	Prio.Nbr	Type
Fa0/2	Desg	FWD	19	128.2	P2p
Fa0/1	Desg	FWD	19	128.1	P2p

- أنظر للصورة هذه من داخل السويتش الرائيسي **Root Bridge** هذه المنافذ لاحظ إنه تاخذ حالة الـ **DP = Designated Port** هذا يعني إنه هذا السويتش الرائيسي و المنافذ في حالة إرسال و استقبال , اما الأن سنقوم بدخول على السويتش الثاني **SW 2** و نقوم بعملية استعراض للمعلومات لنرى ما هي حالة المنافذ .

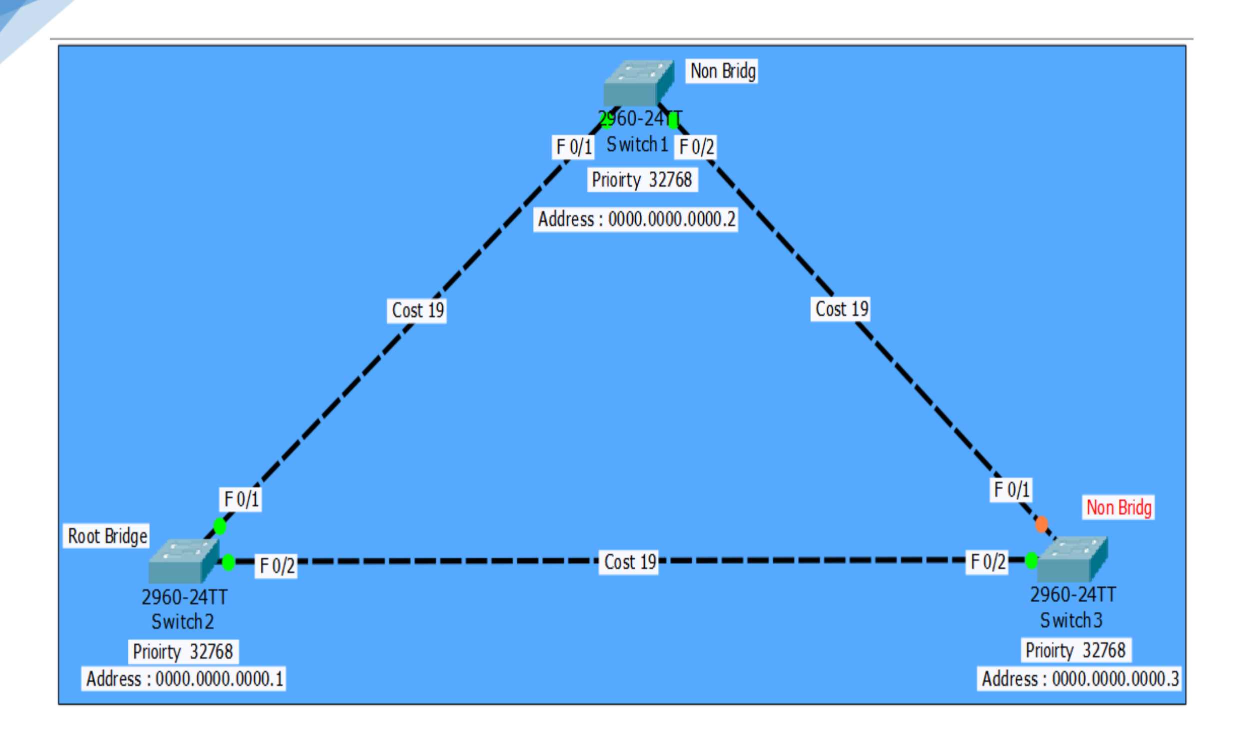
- الأن سنقوم بدخول على السويتش **SW 2** وكتابة الاومر السابق :

SW 2

Interface	Role	Sts	Cost	Prio.Nbr	Type
Fa0/1	Root	FWD	19	128.1	P2p
Fa0/2	Altn	BLK	19	128.2	P2p

- أنظر للصورة هذه من داخل السوتيش الـ **Non Bridg** , أنظر للمنافذ المنفذ الأول **F 0/1** ياخذ حالة الـ **RP = Root Port** و هذا يعني إنه يرسل و يستقبل من السويتش الرائيسي الـ **Root Bridge** بهذه الحالة نعرف إنه يوجد اتصال , اما بنسبه للمنفذ الثاني **F 0/ 2** فهو ياخذ حالة الـ **BP = Block Port** لأنه يخضع تحت امر بروتوكول الـ **STP** و بهذا الشكل لان يحصل عملية دوران البيانات **loop** اما في حال تم تعطيل الينك الأولى فسيتم بشكل تلقائي عملية التحويل الى الينك الثاني ليتم العمل بدل الأول .
- الأن سننتقل لنموذج ثاني متوسط بعض الشيء لنتعرف بشكل اوسع على عملية بروتوكول الـ **STP**.

- هذا النموذج الثاني مكون من ثلاث سويتشات سيتم انتخاب سويتش واحد ليكون السويتش الرائيسي **Root Bridge** و باقي السويتشات ستكون **Non Bridg** كما في النموذج التالي , وسنقوم بدخول على السويتشات لنتعرف على الإعدادات ؟



- لاحظ في النموذج إنه تم اختيار سويتش رائيسي **Root Bridge** و هذا السويتش هو **SW 2** , الأن لنعرف كيف تمت عملية الانتخاب أنظر للنموذج يظهر فيه ثلاث سويتشات قيمة الـ **Prioirty 32768** متساوية في الـ **SW 3** , **SW 2** , **SW 1** في هذه الحالة سيتم تجاوز هذه المرحلة و الانتقال الى المرحلة التالية و هي استكشاف عنوان الماك ادرس للسويتشات أنظر للماك ادرس يوجد اختلاف **SW 1** عنوان الماك ادرس لديه **0000.0000.0000.2** : **MAC Address** و عنوان الماك ادرس لـ **SW 2** **0000.0000.0000.1** : **MAC Address** و عنوان الماك ادرس لـ **SW 3** **MAC Address** : **0000.0000.0000.3** الأن في هذه الحالة سيتم انتخاب السويتش **SW 2** لي إنه يحتوي على اقل ماك ادرس و هو الذي سيكون السويتش الرائيسي **Root Bridge** و باقي السويتشات ستكون **Non Bridg** , اما بنسبه لتكلفة **Cost** ستكون متساوية لي إنه جميع المنافذ تعمل بنفس السرعة و ستكون سرعة المسارات جميعها **Cost 19** كما هو موجود في النموذج .

- الأن سنقوم بدخول على السويتش الأول **SW 1** و نقوم باستعرض المعلومات الخاصة في بروتوكول الـ **STP** :

- **الأن سنقوم بكتابة الاوامر التالية :**

Switch > **enable**

Switch # **show spanning-tree**

SW 1

```
Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/1            Root FWD 19        128.1    P2p
Fa0/2            Desg FWD 19        128.2    P2p
```

- أنظر للصورة هذه من داخل السويتش **SW1** الـ **Non Bridg** , أنظر للمنافذ المنفذ الأول **F 0/1** ياخذ حالة الـ **Root Port = RP** و هذا يعني إنه يرسل و يستقبل من السويتش الرائيسي الـ **Root Bridge** بهذه الحالة نعرف إنه يوجد اتصال مع السويتش الرائيسي **Root Bridge** , اما بنسبه للمنفذ الثاني **F 0/ 2** فهو ياخذ حالة الـ **= DP Designated Port** هذا يدل على إنه متصل في سويتش **SW3** الـ **Non Bridg.**

- الأن سنقوم بدخول على السويتش **SW 2** وكتابة الاومر السابق :

```
Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/1            Desg FWD 19        128.1    P2p
Fa0/2            Desg FWD 19        128.2    P2p
```

- أنظر للصورة هذه من داخل السويتش الرائيسي **SW 2 Root Bridge** و هذه المنافذ لاحظ إنه تاخذ حالة الـ **DP = Designated Port** هذا يعني إنه هذا السويتش الرائيسي و المنافذ في حالة إرسال و استقبال , اما الأن سنقوم بدخول على السويتش الثالث **SW3** و نقوم بعملية استعراض للمعلومات لنرى ما هي حالة المنافذ .

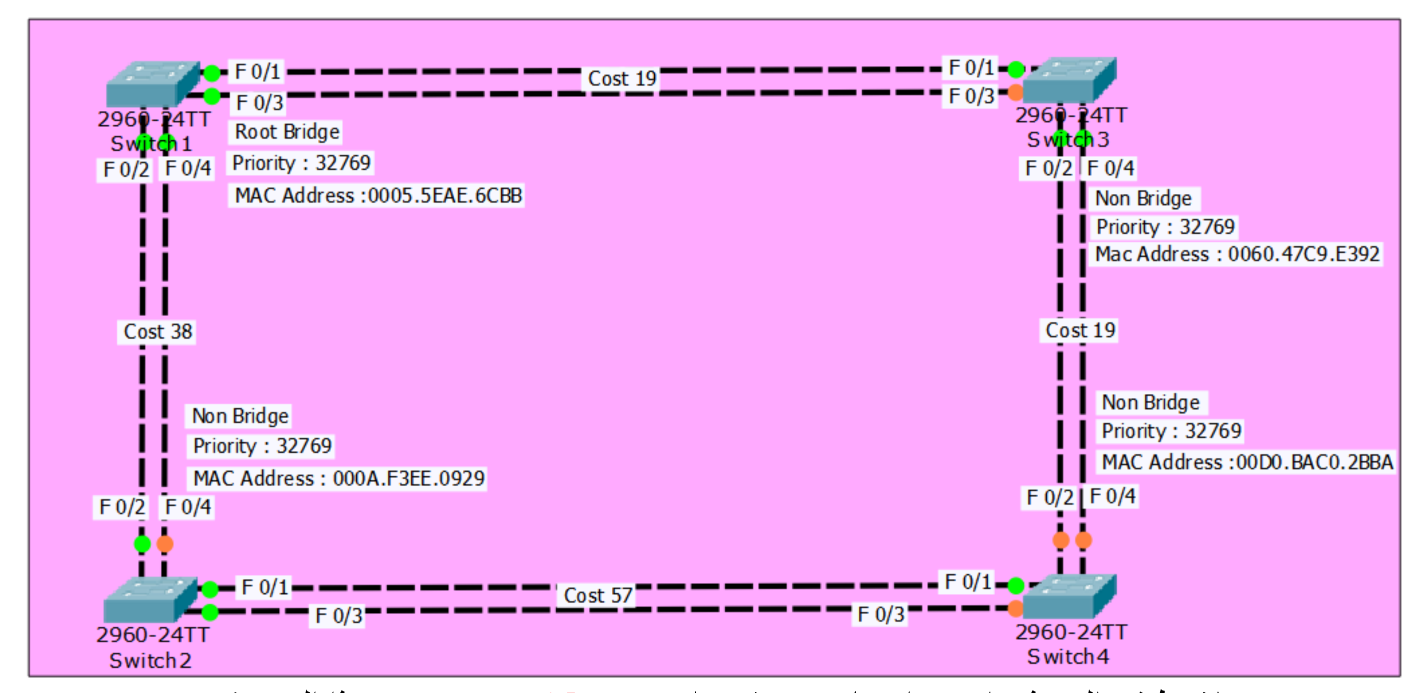
- الأن سنقوم بدخول على السويتش **SW3** وكتابة الاومر السابق :

```
Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/1            Altn BLK 19        128.1    P2p
Fa0/2            Root FWD 19        128.2    P2p
```

- أنظر للصورة هذه من داخل السويتش **SW3** الـ **Non Bridg** , أنظر للمنافذ المنفذ الأول **F 0/1** ياخذ حالة الـ **BP = Block Port** و هذا يعني إنه المنفذ مقفل بشكل مؤقت و لمنع دوران البيانات ما بين السويشات ولكن في حال تعطل أحد الينكات سيتم تشغيل هذه المنفذ بشكل تلقائي بدل من الينك الذي تعطل عن العمل , بنسبه للمنفذ الثاني **F 0/2** لاحظ إنه ياخذ حالة الـ **RP = Root Port** و هذا يعني إنه يرسل و يستقبل من السويتش الرائيسي الـ **Root Bridge** بهذه الحالة نعرف إنه يوجد اتصال مع السويتش الرائيسي **Root Bridge.**

- بهذا النموذج نكون قد فهمنا بشكل متوسط عملية الانتخاب و حالة المنافذ ولكن سأقوم بعمل نموذج آخر اضخم من هذا النموذج لنكون على دراية كاملة بهذا البروتوكول كيف يعمل ولنكون قد فهمنا قاعد بروتوكول الـ **STP.**

- النموذج الثالث مكون من اربعة سويتشات **SW 4 , SW 3 , SW 2 , SW 1** و نلاحظ إنه تم الربط من خلال **2** لينك لكل سويتش , ونلاحظ ايضاً إنه تم ايقاف أحد الينكات في كل سويتش , في هذه الحالة يجب أن نعرف أن بروتوكول الـ **STP** قام بعملية الانتخاب و قام بتحديد لينك واحد لعملية إرسال و استقبال البيانات و تم تحديد سويتش رائيسي **Root Bridge** , بمعنى في هذه الحالة لا يوجد ما يمسى دوران البيانات في الشبكة سنقوم بنظر على النموذج و بعده سأقوم بشرح النموذج بشكل كامل أنظر للنموذج التالي :



- لاحظ في النموذج إنه تم اختيار سويتش رائيسي **Root Bridge** و هذا السويتش هو **SW 1** , الأن لنعرف كيف تمت عملية الانتخاب أنظر للنموذج يظهر فيه اربع سويتشات قيمة الـ **Prioirty 32768** متساوية في الـ **SW 1 , SW 2 , SW 3** , **SW 4** في هذه الحالة سيتم تجاوز هذه المرحلة و الانتقال الى المرحلة التالية و هي استكشاف عنوان الماك ادرس للسويتشات أنظر للماك ادرس يوجد اختلاف **SW 1** عنوان الماك ادرس لديه **MAC Address : 0005.5EAE.6CBB** و عنوان الماك ادرس لـ **SW 2** **MAC Address : 000A.F3EE.0929** و عنوان الماك ادرس لـ **SW 3** **MAC Address : 0060.47C9.E392** و عنوان الماك ادرس لـ **SW4** **MAC Address : 00D0.BAC0.2BBA** , الأن في هذه الحالة سيتم انتخاب السويتش **SW 1** لي لأنه يحتوي على اقل عنوان ماك ادرس و هو الذي سيكون السويتش الرائيسي **Root Bridge** و باقي السويتشات ستكون **Non Bridg** , اما بنسبه لتكلفة **Cost** ستكون متساوية لأن جميع المنافذ تعمل بنفس السرعة و ستكون سرعة المسارات جميعها **Cost 19** كما هو موجود في النموذج , ولكن يجب أن نعلم سيتم حسب التكلفة على حسب المسارات مثل عندما يريد سويتش **SW 3** إرسال رسالة لسويتش **SW**

4 ستخرج البيانات من سويتش **SW 3** و تصل الى **SW 1** السويتش الرائيسي و بعده سيقوم السويتش الرائيسي بإرسال ها للسويتش **SW 2** و سيقوم بإرسال البيانات الى سويتش **SW 4** في هذه الحالة سيتم حسب تكلفة المسارات التي تسير فيها البيانات , و ستكون تكلفة المسار ما بين السويتش **SW 3** و **SW 4** ستكون**Cost 57** كيف تم حسب التكلفة أنظر للنموذج قام بحسب تكلفة المسار الأول الذي يربط ما بين **SW 3** و **SW 1 ستكون القيمة Cost 19** كما في النموذج و بعده سيتم حسب قيمة المسارات التي ما بين **SW 1** و **SW 2** ستكون النتيجة **Cost 38** كما في النموذج موضح و بعده سيتم حسب التكلفة التي تربط ما بين **SW 2** و **SW 4** ما إضافة الـ **Cost 38** ستكون النتيجة **Cost 57** هذه النتيجة النهائية .

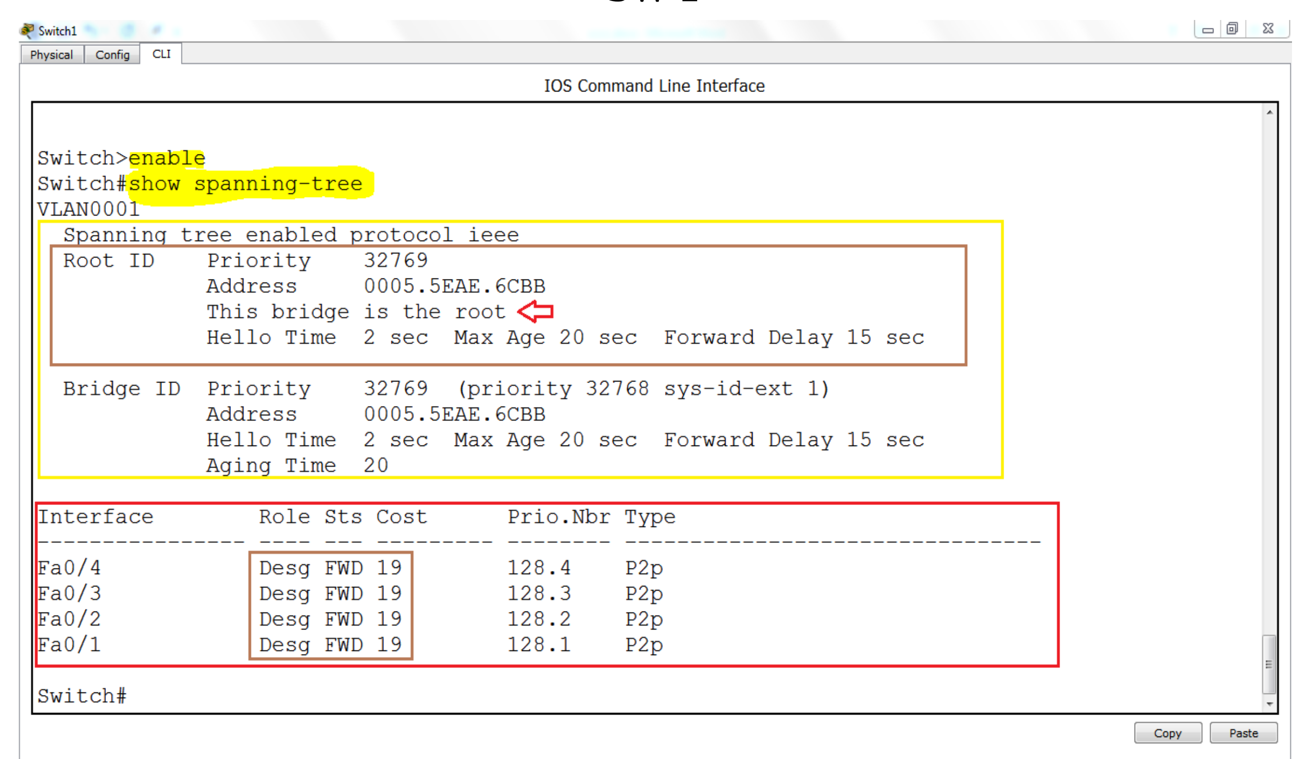
- الأن سنقوم بدخول على السويتش الأول **SW 1** و نقوم باستعرض المعلومات الخاصة في بروتوكول الـ **STP** :
- **الأن سنقوم بكتابة الاوامر التالية :**

Switch > **enable**

Switch # **show spanning-tree**

- أنظر للصورة التالية من داخل السويتش الرائيسي **SW 1** **Root Bridge** لاحظ إنه جميع المنافذ تاخذ حالة الـ **DP = Designated Port** هذا يعني إنه هذا السويتش الرائيسي و المنافذ في حالة إرسال و استقبال , اما الأن سنقوم بدخول على السويتش الثالث **SW 2** و نقوم بعملية استعراض للمعلومات لنرى ما هي حالة المنافذ.
- الأن سنقوم بدخول على السويتش **SW 2** وكتابة الاومر السابق :

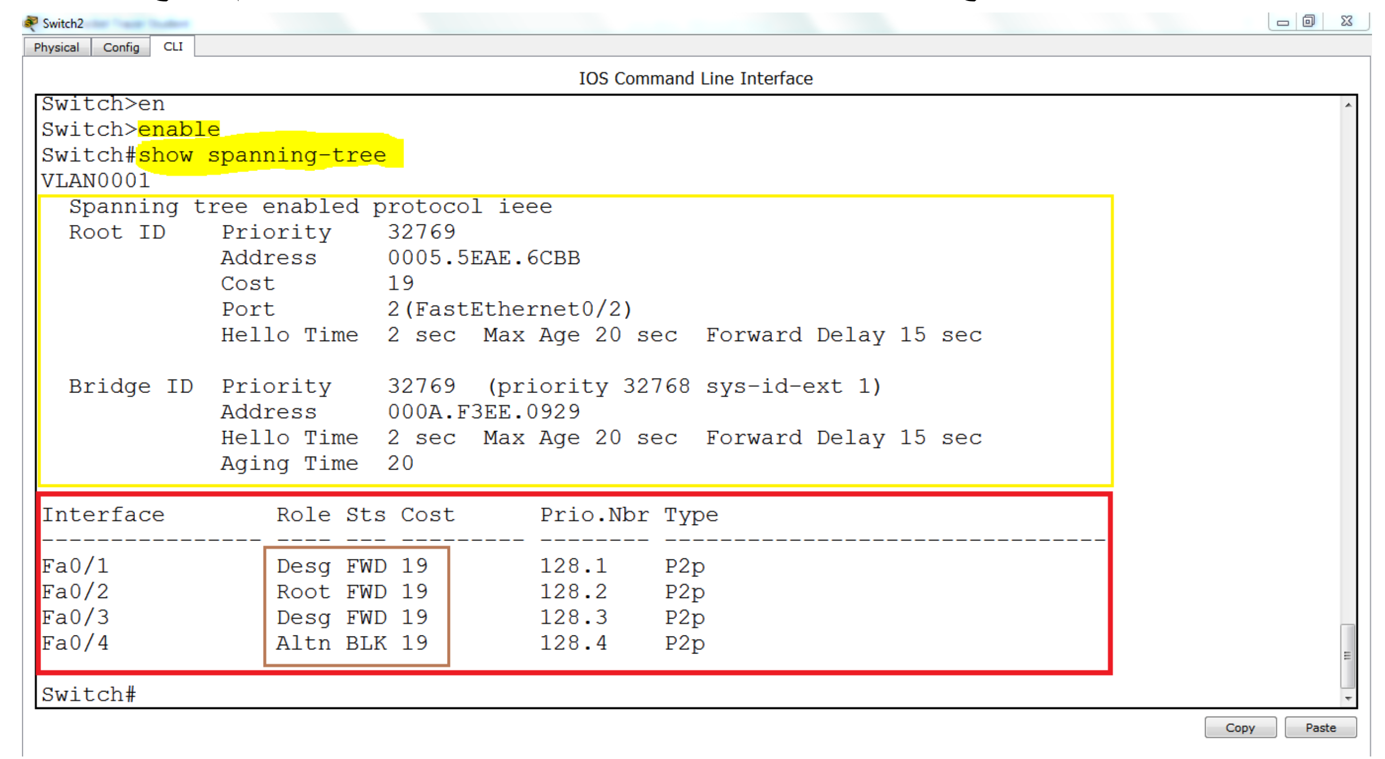
SW 1



- أنظر للصورة التالية من داخل السويتش الثاني **SW 2 Non Bridge ,** و المنافذ لاحظ إنه تاخذ حالة مختلفة هذا يدل على إنه سويتش مرتبط باكثر من سويتش سأقوم بشرح هذه المنافذ .

SW 2

- لاحظ إنه يوجد اربع منافذ متصلة كل منفذ ياخذ حالة مختلفة عن الآخر سأقوم بشرح



```
Switch>en
Switch>enable
Switch#show spanning-tree
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    32769
             Address     0005.5EAE.6CBB
             Cost        19
             Port        2(FastEthernet0/2)
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32769  (priority 32768 sys-id-ext 1)
             Address     000A.F3EE.0929
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/1            Desg FWD 19        128.1    P2p
Fa0/2            Root FWD 19        128.2    P2p
Fa0/3            Desg FWD 19        128.3    P2p
Fa0/4            Altn BLK 19        128.4    P2p

Switch#
```

المنافذ المتصلة في السويتشات .

Fa0/1 Desg FWD هذا المنفذ متصل في السويتش الرابع **SW 4** و في حالة إرسال و استقبال ما بين السويتش الرائيسي **Root Bridge** و السويتش **Non Bridge**.

Fa0/2 Root FWD هذا المنفذ متصل بسويتش الأول الرائيسي **SW 1 Root Bridge**.

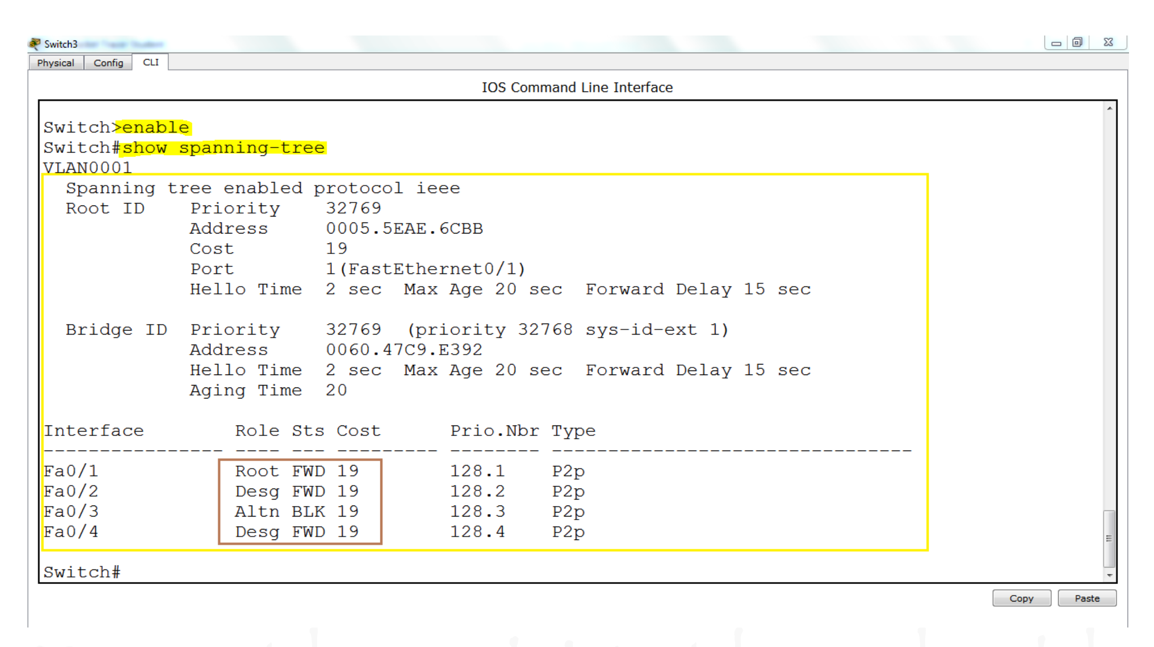
Fa0/3 Desg FWD هذا المنفذ متصل بسويتش الرابع **SW 4** و في حالة إرسال.

Fa 0/4 Altn BLK هذا المنفذ المعطل بشكل مؤقت و متصل بسويتش الأول الرائيسي **Root Bridge SW 1**.

- في هذا النموذج قمت بعمل اكثر من توصيل لتعقيد الشبكة و فهمها بشكل ممتاز لنتعرف على كيف يعمل بروتوكول الـ **STP** و نتعرف على كيفية حل مشكلة دوران البيانات و ايضاً اخذ الاحتياط من عدم تعطل أحد الينكات , سيتم تشغيل لينك تم ايقافه بشكل مؤقت ليعود تشغيله ايضاً بشكل تلقائي من غير تدخل بهذا الشكل نكون قد تجاوزنا مشكلة دوران البيانات و تعطل اي لينك بشكل مفاجئ .

- الأن سنقوم بدخول على السويتش **SW 3** وكتابة الاومر السابق :
- أنظر للصورة التالية من داخل السويتش الثالث **SW 3** **Non Bridge ,** و المنافذ لاحظ إنه تاخذ حالة مختلفة هذا يدل على إنه سويتش مرتبط باكثر من سويتش سأقوم بشرح هذه المنافذ .

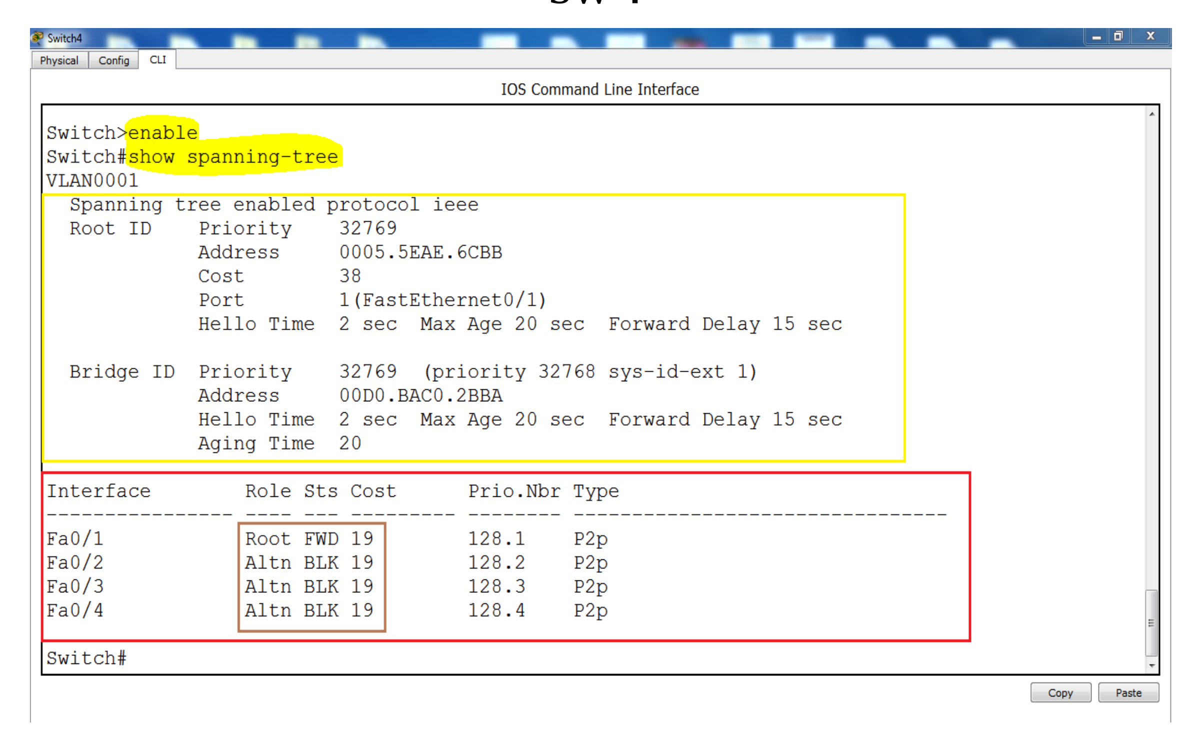
SW 3



- لاحظ إنه يوجد اربع منافذ متصلة كل منفذ ياخذ حالة مختلفة عن الآخر بنفس حالة السويتش الثاني لأنه ساقوم باعدة الشرح لي لأنه نفس حالة السويتش الثاني .

- الأن سنقوم بدخول على السويتش **SW 4** وكتابة الامر السابق :

SW 4



- لاحظ الصورة التالية من داخل السويتش الرابع **SW 4** و يظهر لنا اربع منافذ بينم يوجد منفذ واحد فقط يعمل بحالة و باقي المنافذ تاخذ حالة اخرى سأقوم بشرحهم .

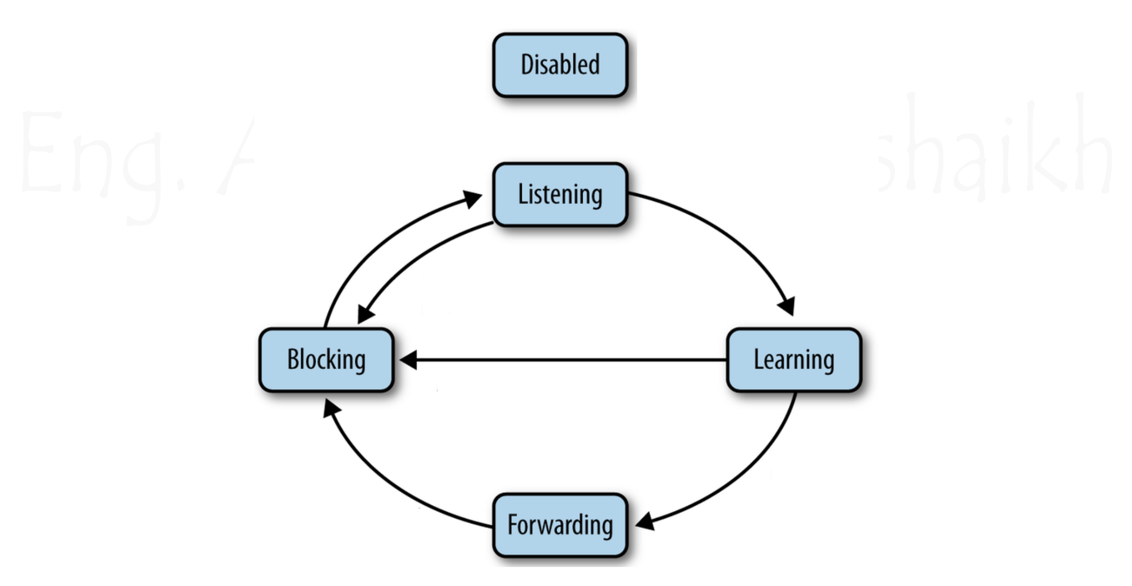
Fa0/1 Root FWD هذا المنفذ يدل على إنه متصل مع السويتش الرائيسي **SW 1** **Root Bridge**.

Fa 0/4 Altn BLK هذا المنفذ المعطل بشكل مؤقت و متصل بسويتش الأول الرائيسي **Root Bridge SW 1** و في باقي السويتش الـ **Non Bridge**.

- بهذا الشكل نكون قد تم الانتهاء من بروتوكول الـ **STP** ولكن يجب أن نعلم إنه تم تطوير هذا البروتوكول و تم ايضاً إضافة بعض الإضافة الخاص في هذا البروتوكول و تم تطويره لعددة بروتوكولات سأقوم بذكره و الشرح عنه لنكون على معرفة كامل في بروتوكول الـ **STP** .

مرحلة قرارات المنافذ في السويتشات

STP switch port states



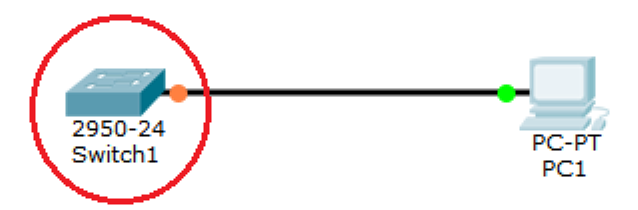
- مرحلة قرارات المنافذ في السويتش تاخذ **30** ثانية لي عملية استقرار المنفذ و في هذا الوقت الذي ياخذه المنفذ يكون على عملية تهيئة نفسه ليعمل بشكل صحيح و يبداء في العمل و يضياء بالون الاخضر , و تبداء هذه العملية بعددة خطوات سأقوم بذكرها .

1- **Blocking** المنفذ في حالة اغلاق سيتم الانتقال للمرحلة الثانية
2- **Listening** المنفذ في حالة استماع ماذا سيكون في هذه المرحلة سيتم تحديد نوع المنفذ
3- **Learning** المنفذ في حالة تجهيز نفسه ليستلم وظيفته
4- **Forwarding** المنفذ في حالة إرسال و استقبال و هذه المرحلة بعد تعين نوعه المنفذ
5- **Disabled** المنفذ في حالة تعطل

- بعد أن تعرفنا على حالة المنافذ سأقوم بشرح كل حالة من هذه الحالة بشكل منفصل مع ذكر امثلة على كل حالة لنفهم حالة المنافذ بشكل ممتاز .

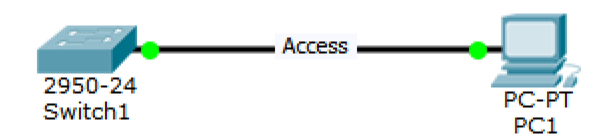
Blocking : هذه حالة المنفذ عند أول مرحلة تشغيل له سيكون بشكل مغلق و عند تشغيله سيتم الانتقال للمرحلة الثانية.

كما في الصورة التالية المنفذ مضيباء بالون البرتقالي هذا يعني إنه الحالة **Blocking** و ياخذ المنفذ وقت **30** ثانية لعملية استقرار المنفذ أنظر للصورة التالية :



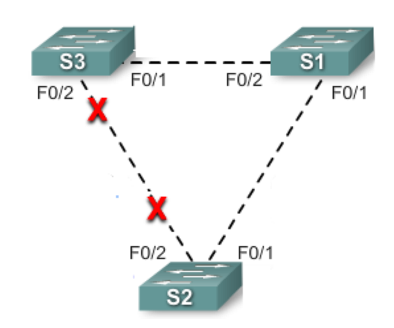
Listening : هذه حالة المنفذ يكون يستمع ماذا سيكون نوعها هل سيكون **Access** أو **Trunk** و هذه الحالة تاخذ **15** ثانية من عملية الاستماع من المنفذ المقابل ما هو نوعها و بعده ينتقل للمرحلة الثالثة .

Learning : هذه حالة المنفذ بعد تحديد نوعه و وظيفته سياخذ وقت **15** ثانية من عملية التجهيز و بعد أن قام يقوم بتحديد المنفذ إنه سيكون من نوع **Access** و هذه المنفذ متصل في جهاز حاسوب كما في الصورة التالي و سيقوم السويتش بتسجيل عنوان الماك ادرس في جدول العناوين الفيزيائية .



Forwarding: في هذه الحالة المنفذ تم استقراره و الأن في حالة إرسال و استقبال بشكل طبيعي.

Disabled: هذه حالة المنفذ عندما نريد اغلاقها ولا نريد العمل عليه مثل نريد اقفال منفذ معين بشكل كامل حتى ولو تم توصيله في أحد الأجهزة لن يعمل ابداً.



Optimizing Spanning Tree Protocol

تطوير بروتوكول الـ STP



- مرحلة تطوير بروتوكول الـ **STP** كانت لحل كثير من المشاكل التي تحصل في الشبكة مثل الوقت الزائد في استقرار حالة المنافذ الخاصة في السويتشات , و تحسين اداء الشبكة بشكل عام مثل عملية انتخاب السويتش الرائيسي في بروتوكول الـ **STP** , سأقوم بذكر التحديثات التي حصلت على هذا البروتوكول .

1- Port Fast
2- Uplink Fast
3- Backbone Fast
4- RLQ BPDU = Root Link Query

Port Fast: هذه الخاصية التي تم تطويرها لتحسين عملية المنافذ، وظيفة هذه الخاصية تجاهل حالة الانتظار التي تاخذ **30 sec** ثانية في حالة استقرار المنفذ و هي **Listening**, و **Learning** و هذه الخاصية تعمل بشكل مباشر مثل عندما ا نقوم بتبديل لينك أو ربط جهاز بمنفذ السويتش لان ينتظر **30 sec** ثانية بل سيتم الربط بشكل مباشر من دون انتظار و هذه الخاصية مهم جداً جداً.

- **ملاحظة مهم جداً جداً جداً :** يجب أن نعلم إنه هذه العملية فقط يتم تطبيقها على منافذ الـ **Access** بمعنى المنافذ التي تتصل فيها أجهزة حاسوب فقط لا غير , ولا يجب أن نقوم بعمل هذه الخاصة على المنافذ التي تربط السويتشات مع بعضها البعض .

Uplink Fast : هذه الخاصية مهم جداً ايضاً و وظيفة هذه الخاصية إنه تقوم بعددة وظائف، تقوم بزيادة السرعة في الينك و تفيد ايضاً في حالة تم تعطيل أحد الينكات سيتم التحويل بسرعة مباشرة جداً و من دون انتظار سيتم تبديل الينك الذي تعطل بلينك يعمل.

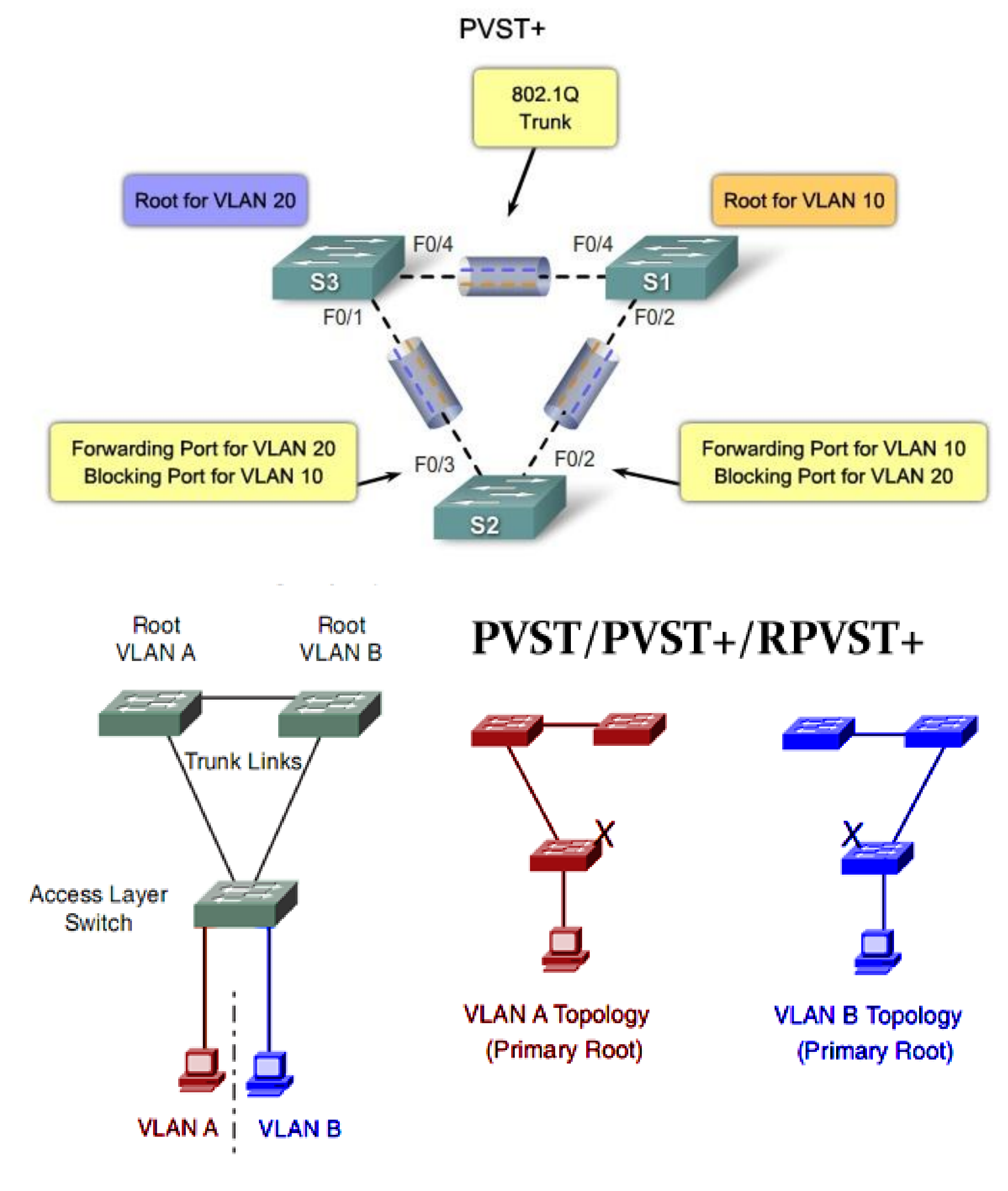
ملاحظة مهم جداً جداً جداً : يجب أن نكون على معرفة إنه إذا تم تفعيل هذه الخاصية على السوتيش الذي نريده لي يدخل هذه السويتش في عملية انتخاب السويتش الرائيسي .

Backbone Fast : هذه الخاصية تفيد عندما ا تكون لدنيا عدة سويتشات و تم انتخاب سويتش رئيسي، و عندما ا يتوقف السويتش الرئيسي عن العمل ستبداء السويتشات بإرسال رسالة الـ **RLQ BPDU** لعملية الاستكشاف هل يوجد سويتش رئيسي في الشبكة أو لا و أن وجد سيتم تعديل المسارات اما في حال لما يجد سيتم معاودة انتخاب سويتش رئيسي من جديد.

Per Vlan Spanning Tree

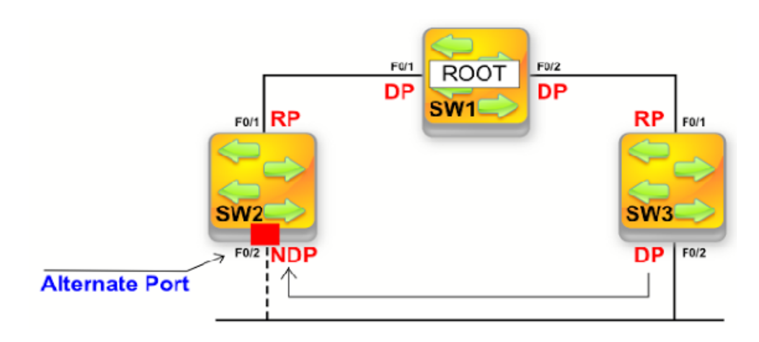
PVST

PVST: هو عبارة عن بروتوكول خاص بشركة سيسكو و يعمل فقط على أجهزة سيسكو، و هذه مجموعة من البروتوكولات ولكن سأقوم بذكر هذا البروتوكول **PVST**، و فكرة هذا البروتوكول إنه يعمل على اساسيات تطبيقات بروتوكول الـ **STP** على مستوى الشبكة الافتراضي الوهمية **Vlan** و يقوم هذا البروتوكول على تقسيم هذه الشبكات مثل كل شبكة تملك تصميمها الخاص فيها و مساراتها الخاصة فيها حيث يدعم ايضاً عملية توزيع الحمل ما بين الينكات أو نستطيع أن نقول الـ **Load Balancing**.



Rapid Spanning Tree Protocol

RSTP



RSTP : هذا البروتوكول تم تطويره على اساسيات بروتوكول الـ **STP** بمعنى إنه مطور منه و يرمز لهذا البروتوكول برمز **802.1w**، و هذا البروتوكول مهتم بسرعة و تم اختصار الوقت الذي كان يعتمد عليه بروتوكول الـ **STP** كان يعتمد على وقت **20 Sec** ثانية و تم اختصارهم في بروتوكول الـ **RSTP** لـ **6 Sec** ثواني، ولكن هو نفس وظيفة بروتوكول الـ **STP** يقوم بانتخاب سويتش رئيسي **Root Bridge**.

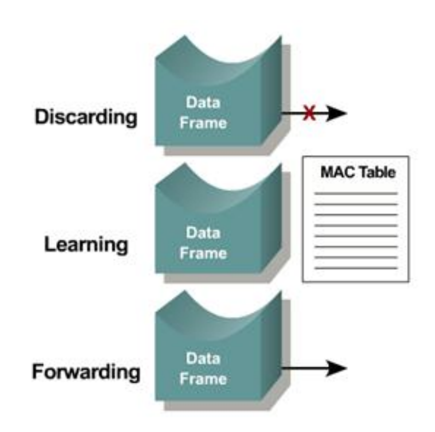
- الأن اريد أن اوضح الحالة التي يعتمد عليه الـ **RSTP** .
- قبل أن نبداء اريد أن اوضح اشياء بسيطة جداً لنتعرف و نفهم ما هي الحالة التي تم اختصاره من بروتوكول الـ **STP** .
- هذه الحالة التي يعتمد عليها بروتوكول الـ **STP** خمس حالة و تم اختصاره في بروتوكول الـ **RSTP** و اصبحت ثلاث حالة سأقوم بذكرهم .

هذه الحالة قمنا بتعرف عليها و شرح مسبقاً STP switch port states

1- Blocking , 2- Listening , 3- Learning , 4- Forwarding , 5- Disabled

- **RSTP switch port states**

في بروتوكول الـ **RSTP** تم دمج حالة المنافذ الخاص في الـ **Blocking** و **Listening** بحالة واحدة و هي الـ **Discarding** و كما نعرف أن الـ **Listening** لديه وقت معين مكون من **15 Sec** ثانية .

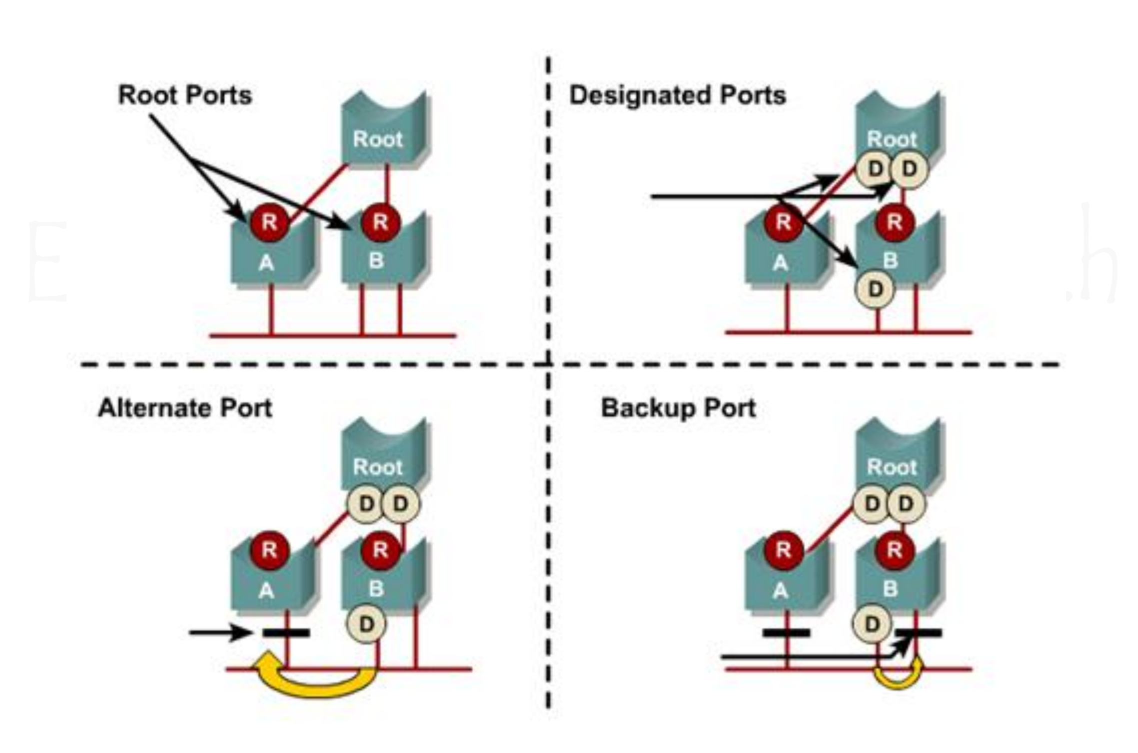


1- **Discarding** حالة المنفذ معطل لا يتسقبل ولا يرسل اية بيانات
2- **Learning** تعلم العناوين و تسجيلها في جدول العناوين الموجود في السويتش
3- **Forwarding** عملية التصفية والإرسال

- **RSTP bridge port roles** حالة المنافذ في بروتوكول الـ

1- **Root** هذه حالة المنفذ صاحب التكلفة الاقل و ايضاً يكون متصل في السويتش
2- **Designated** هذه حالة المنفذ التي داماً تكون في حالة إرسال و استقبال
3- **Alternate** هذه حالة المنفذ الذي يكون بديل لمنفذ الـ **Root**
4- **Backup** هذه حالة المنفذ الذي يكون متصل عليه لينك احتياطي
5- **Disabled** حالة المنفذ المعطل بشكل يدوي

كما في الصورة التالية

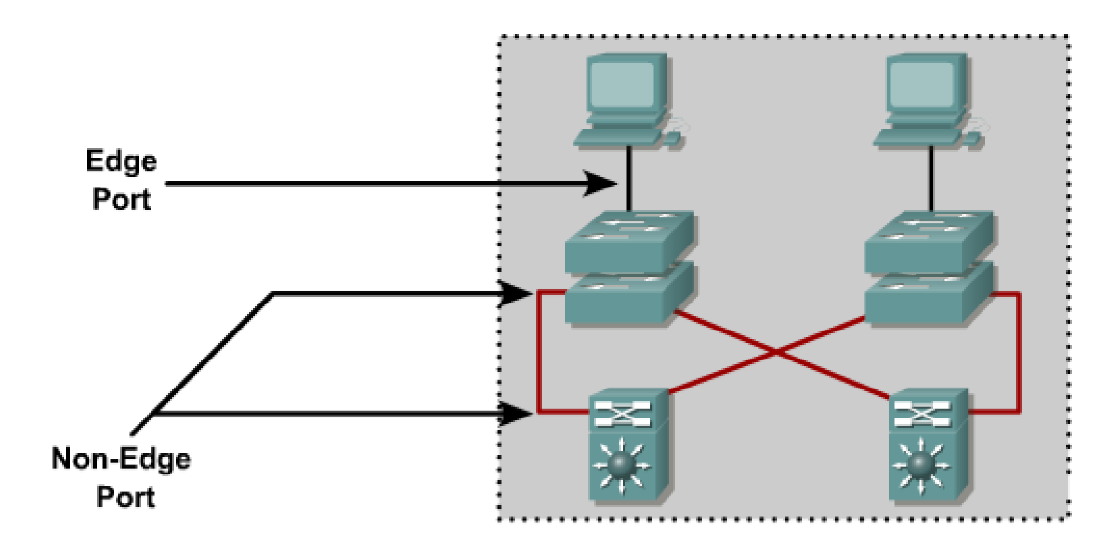


أنواع طريق الربط في بروتوكول الـ RSTP

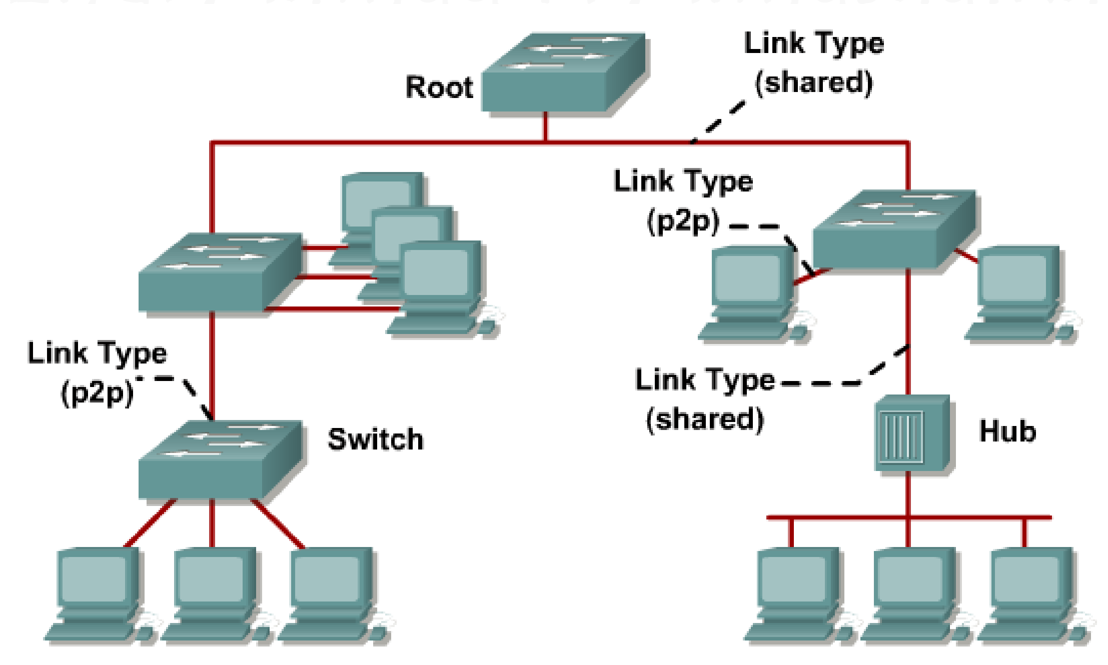
- يوجد ثلاث حالة على أنواع الربط ما بين السويتش و الأجهزة الآخر سأقوم بذكرهم:

1- **Point to Point** هذه النوع من الربط هو ربط سويتش في سوتيش اخر
2- **Shared** هذا النوع من الربط يكون متصل مثل بجهاز هاب
3- **Edge** هذا النوع من الربط يكون متصل بجهاز حاسوب أو خادم أو طابعة

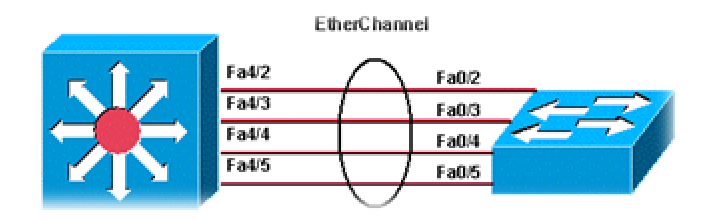
كما في الصورة التالية



Link Type

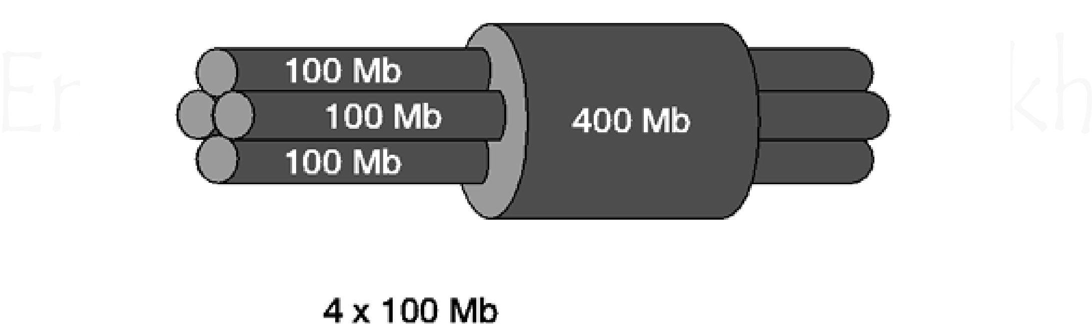


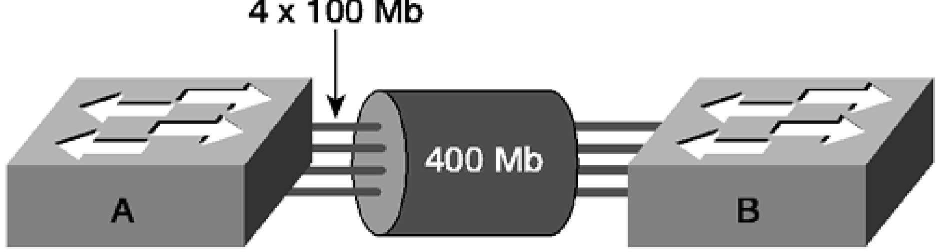
Port Channel



- **Port Channel**: هي عبارة عن تقنية يتم فيه دمج اكثر من منفذ موجودين على نفس جهاز السويتش ليتم العمل و كإنهم منفذ واحد بسرعة عالة جداً.

• مثال على هذه التقنية لنفترض أن لدينا سويتشان يربط ما بينهم عدة لينكات في هذه الحالة من الطبيعي جداً أن نعرف إنه يعمل بروتوكول الـ **STP** و سيقوم بتشغيل لينك واحد و ايقاف باقي الينكات لمنع عملية الدوران الـ **Loop** في السويتشات , في هذه الحالة لان نستفيد من الينكات و البورتات التي تم توقيفها بشكل مؤقت ولكن ماذا لو قمنا بعمل تقنية الـ **Port Channel** لتقوم بدمج هذه الينكات, و المنافذ في بعضها البعض لتعمل و كإنه لينك واحدة و منفذ واحد, و مع العلم إنه سيتم دمج كل منفذ بسرعته الخاصة ليصبح سرعة المنفذ و الينك اضعاف السرعة الطبيعية كما في الصورة التالية.





- لاحظ في الصورة إنه يوجد اربع لينكات متصلين في اربع منافذ و كل منفذ يعمل بسرعة **100 Mb** و عند تشغيل تقنية الـ **Port Channel** سيتم دمج الاربع منافذ و كإنهم منذ واحد و سيتم ايضاً دمج السرعة لتصبح **400 Mb** كما هو وضح في الصورة اعلى .

- **معلومات ما قبل الدخول لتطبيق هذه التقنية يجب أن نعرفها :**

- يجب أن تكون جميع المنافذ المتصله فيها الينكات من نوع الـ **Trunk**.

- ويجب أن نعلم إنه هذه التقنية تعمل في الطبقة الثانية و الثالث من الطقبات السبعة **OSI**.

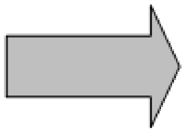
- يجب أن تكون سرعة المنافذ متساوية لتعمل بشكل صحيح , مثل **100 mb / 100 mb** ولكن إذا كانت المنافذ غير متساوية مثل **10 mb /100 mb / 1000 mb** , ستحصل بعض المشاكل في عملية توزيع الترافيك لي لأنه المنافذ غير متساوية .

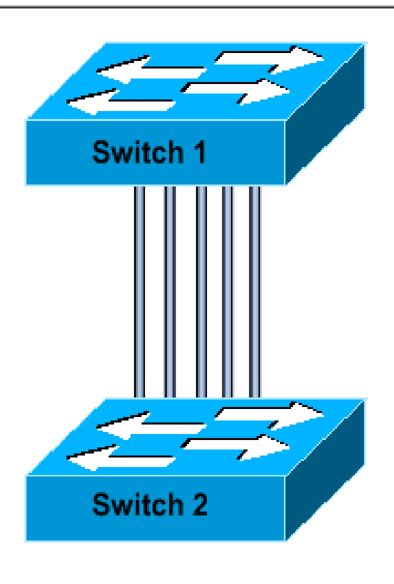
- هذه التقنية له الكثير من الفوائد و تحل كثير من المشاكل التي تصدفنا مثل توزيع الترافيك و عدم انقطاع الاتصال ما بين السويتشات , و تكون السرعة اكبر بكثير من أن يكون منفذ واحد يقوم بعملية إرسال و استقبال البيانات .

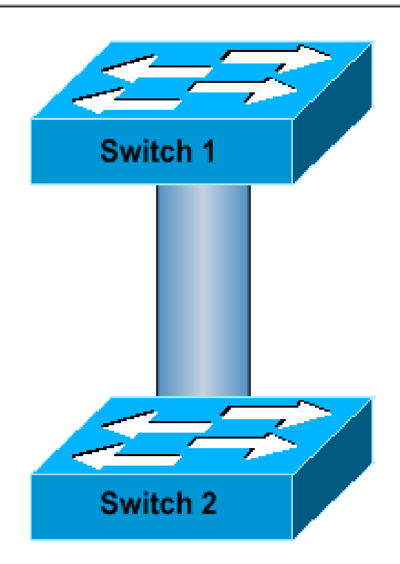
- يعمل مع السيرفرات بمعنى نستيطع دمج اكثر من لينك ما بين السيرفر و السوتيش .

- يعمل ايضاً مع الراوترات مثل يكون لدينا راوترين متصلين باكثر من لينك .

- يجب أن نعلم أن هذه التقنية عند تطبيقها تتحول المنافذ الى حالة الـ **Logical Port** و تصبح جميع المنافذ منفذ واحد في نظر بروتوكول الـ **STP** اما في الحقيقة هي عدة منافذ , هذا يعني إنه في داخل السويتش سيتم تحويل المنافذ الـ حالة الـ **Logical Port** و في الواقع هي **Physical Port** كما في الصورة التالية .

Physical View		Logical View
Multiple ports are defined as being part of an EtherChannel group		The different subsystems running on the switch see only one logical link





البروتوكولات التي تدعم هذه التقنية Port Channel Protocols

1- Port Aggregation Protocol (PagP) - Cisco

هذا البروتوكول من تطوير شركة سيسكو و هو خاص فقط في أجهزة سيسكو

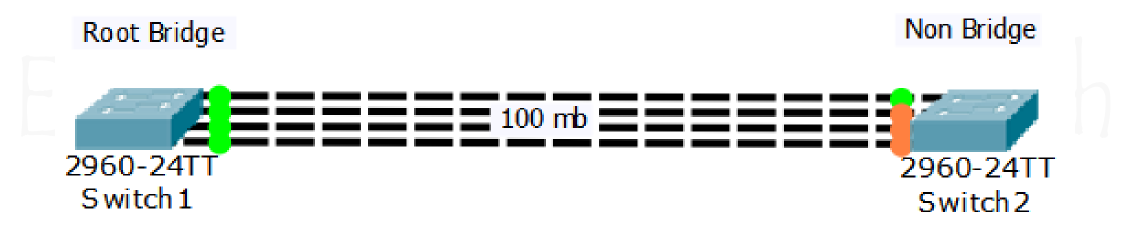
2- Limk Aggregation Control Protocol (LACP) - IEEE 82.1AD

هذا البروتوكول من مؤسسة الـ **IEEE** و هو يعمل مع الأجهزة المختلفة غير سيسكو .

و هذا الجدول يوضح الفرق ما بين هذه البروتوكولات في عملية الاتصال ما بين المنافذ .

protocol	Link A mode	Link B mode	Negotiation result
PAGP	Auto	Auto	No negotiation
	Auto	Desirable	Negotiation successful
	Auto	On	No negotiation
	Desirable	Desirable	Negotiation successful
LACP	Passive	Passive	No negotiation
	Passive	Active	Negotiation successful
	Passive	On	No negotiation
	Active	Active	Negotiation successful

- الأن سنقوم بعمل تطبيق على النموذج التالي :



- لاحظ أن هذا النموذج يحتوي على سويتشان و يربط ما بينهم اربعة لينكات بسرعة **100 mb** لكل لينك , ويجب أن تلاحظ إنه تم تشغيل بروتوكول الـ **STP** بشكل تلقائي و تم انتخاب سويتش رائيسي **Root Bridge** .
- الأن سنقوم بعمل إعدادات تقنية الـ **Port Channel** و نقوم بدمج المنافذ و الينكات مع بعضهم البعض لتصبح السرعة **400 mb** و تعمل جميع المنافذ و كإنهم منفذ واحد بسرعة واحدة .

Port Channel Configuration الإعدادات

Switch > **enable**

Switch # **config t**

Switch (config) # **interface range fastethernet 0/1 – 4**

Switch (config-if-range) # **channel-group 1 mode desirable**

Switch (config-if-range) # **channel-protocol pagp**

- الأن سنقوم بدخول على السويتش الأول **SW 1** و عمل الإعدادات سنقوم بكتابة الاوامر التالية :

Switch > **enable**

Switch # **config t**

Switch (config) # **interface range fastethernet 0/1 – 4**

Switch (config-if-range) # **channel-group 1 mode desirable**

Switch (config-if-range) # **channel-protocol pagp**

Switch (config-if-range) # **end**

Switch # **copy running-config startup-config**

بهذه الإعدادات نكون قد قمنا بدمج المنافذ و الينكات على السويتش الأول سنقوم بدخول على السويتش الثاني **SW 2** .

- الأن سنقوم بدخول على السويتش الأول **SW 2** و عمل الإعدادات سنقوم بكتابة الاوامر التالية :

Switch > **enable**

Switch # **config t**

Switch (config) # **interface range fastethernet 0/1 – 4**

Switch (config-if-range) # **channel-group 1 mode desirable**

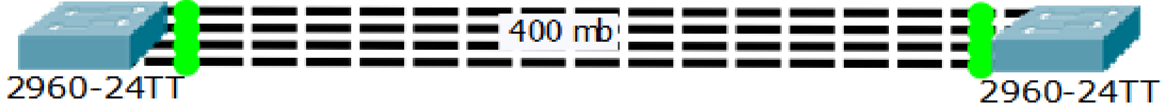
Switch (config-if-range) # **channel-protocol pagp**

Switch (config-if-range) # **end**

Switch # **copy running-config startup-config**

بهذه الإعدادات نكون قد قمنا بدمج المنافذ و الينكات على السويتش الثاني **SW 2** .

- الأن أنظر للنموذج بعد أن قمنا بعمل الإعدادات على السويتشات تم تحويل المنافذ الاربعة الى اللون الاخضر و هذا يدل على إنه جميع المنافذ تعمل بنفس الوقت و جميع المنافذ و الينكات اصبحت منفذ واحد و لينك وحدا بسرعة **400 mb**.



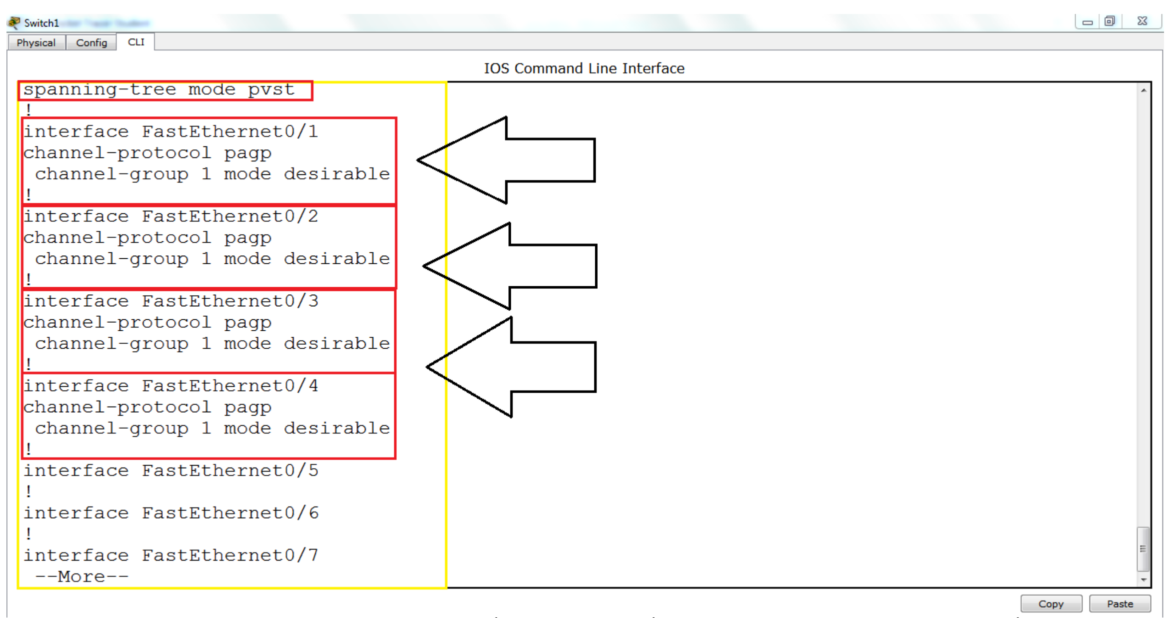
- الأن سنقوم بدخول على السويتش الأول **SW 1** لننظر على الإعدادات و حالة السويتش بعد عملية تطبيق تقنية الـ **Port Channel** سنقوم بكتابة الاوامر التالية .

- سنقوم بكتابة الأمر التالي لعرض ملف التشغيل الذي يحتوي على الإعدادات :

Switch > **enable**

Switch # **show running-config**

SW 1



- لاحظ الأن نحن في داخل السويتش الأول **SW 1** أنظر للمنافذ الموجودة من منفذ **F 0/1 , F 0/2 , F0/3, F0/4** سنجد إنهم يخضعون تحت تقنية الـ **channel-protocol pagp** هذا يدل على إنهم يعملون في منفذ واحد و لينك واحدة و بسرعة واحدة .

- الأن سنقوم بكتابة الأمر التالي لنرى إعدادات الـ **STP** :

Switch # **show spanning-tree**

```
Switch#show spanning-tree
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    32769
             Address     0000.0C4B.15C5
             Cost        7
             Port        27(Port-channel 1)
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32769  (priority 32768 sys-id-ext 1)
             Address     0005.5E29.EA8A
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Po1              Root FWD 7         128.27   Shr
```

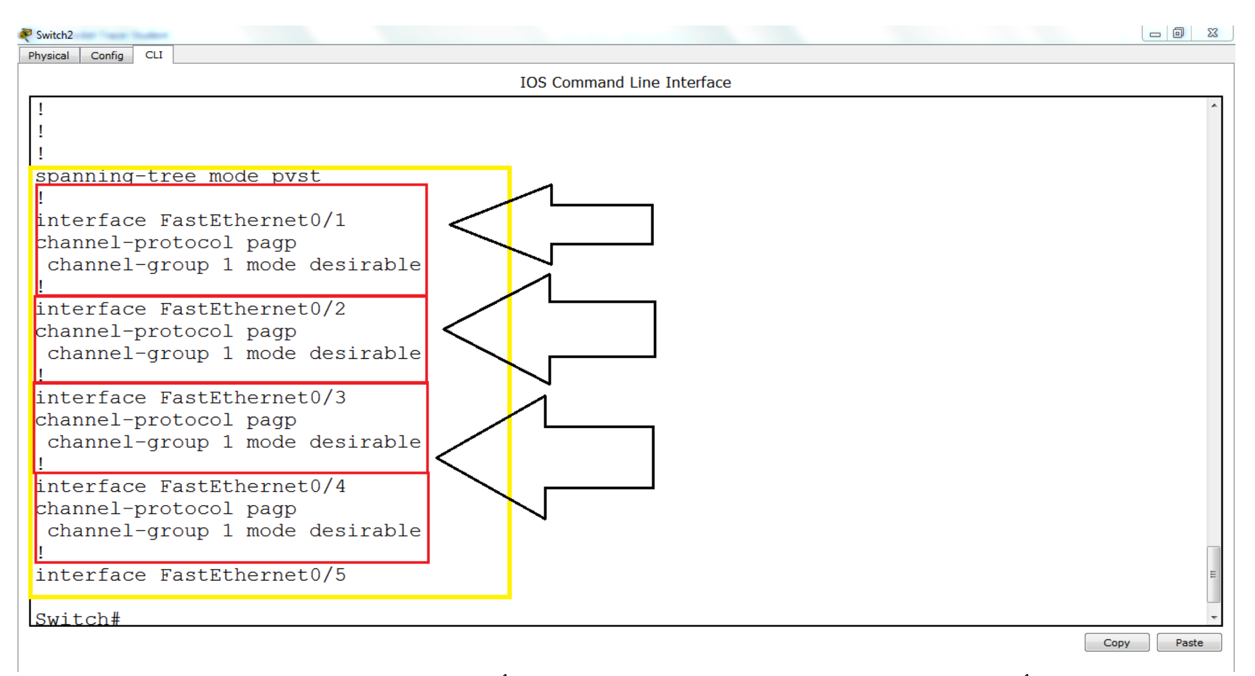
- لاحظ الأن تم عرض إعدادات **STP** للسويتش الأول **SW 1** سنرى إنه هو السويتش الرائيسي **Root Bridge** , و سنرى ايضاً إنه يعمل بمنفذ واحد هذا يدل على إنه يعمل بتقنية الـ **Port Channel** و تم دمج المنافذ الاربعة مع بعضهم البعض و اصبحوا منفذ واحد يعمل بسرعة **400 mb** و جميع الينكات تعمل وكإنه لينك واحد.

- الأن سنقوم بدخول على السويتش الثاني **SW 2** لننظر على الإعدادات و حالة السويتش بعد عملية تطبيق تقنية الـ **Port Channel** سنقوم بكتابة الاوامر التالية .
- سنقوم بكتابة الأمر التالي لعرض ملف التشغيل الذي يحتوي على الإعدادات :

Switch > **enable**

Switch # **show running-config**

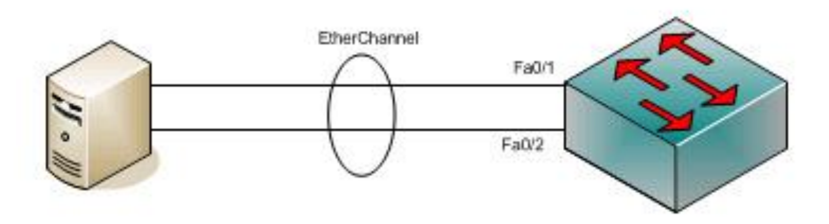
SW 2



- لاحظ الأن نحن في داخل السويتش الثاني **SW 2** أنظر للمنافذ الموجودة من منفذ **F 0/1 , F 0/2 , F0/3, F0/4** سنجد إنهم يخضعون تحت تقنية الـ **channel-protocol pagp** هذا يدل على إنهم يعملون في منفذ واحد و لينك واحدة و بسرعة واحدة .
- الأن سنقوم بكاتبة الأمر التالي لنرى إعدادات الـ **STP** :

- لاحظ الأن تم عرض إعدادات **STP** للسويتش الثاني **SW 2** سنرى إنه هو السويتش **Non Bridge** , و سنرى ايضاً إنه يعمل بمنفذ واحد هذا يدل على إنه يعمل بتقنية الـ **Port Channel** و تم دمج المنافذ الاربعة مع بعضهم البعض و اصبحوا منفذ واحد يعمل بسرعة **400 mb** و جميع الينكات تعمل وكإنه لينك واحد.

Ether Channel

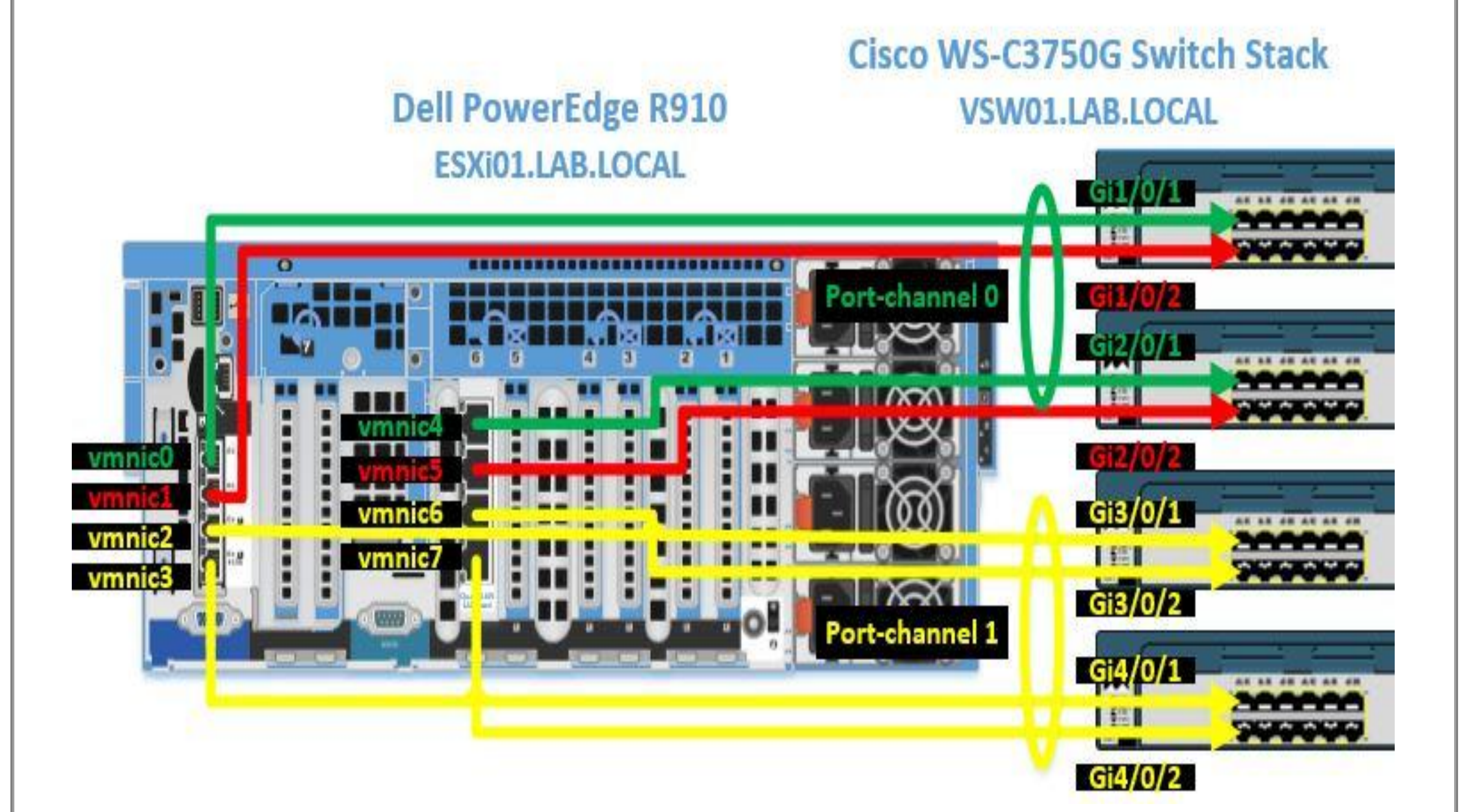


Ether Channel: هذه التقنية شبيها لتقنية الـ **Port Channel** ولكن يوجد اختلاف بسيط ما بينهم سأقوم بتوضيح الفرق ما بينهم و كل واحدة ما هي وظيفتها.

Port Channel: هذه التقنية تعمل ما بين السويتشات.

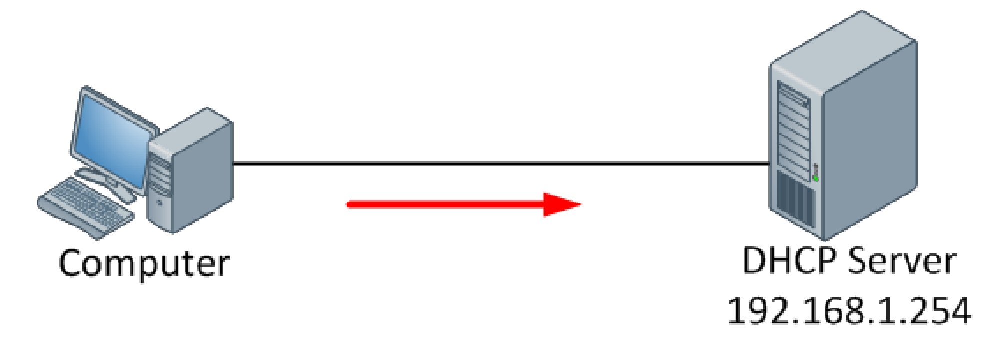
Ether Channel : هذه التقنية تعمل ما بين سويتش و سيرفر حيث يوجد سيرفرات مركب عليه اكثر من كرت شبكة يحتوي على عدة منافذ مما نقوم بربط هذه المنافذ في لينكات و ربطهم في سويتش و نقوم بدمجهم في بعضهم البعض لبتقى تعمل مثل تقنية الـ **Port Channel** .

- أنظر للصورة التالية توضح طريق الربط بتقنية الـ **Ether Channel** يوجد في هذه الصورة جهاز سيرفر و مركب عليه اكثر من كرت شبكة بعدة منافذ و تم ربطهم في سويتش سيسكو وعمل الإعدادات لتقنية الـ **Ether Channel** ليعملوا بمنفذ واحد كما في الصورة.



Dynamic Host Configuration Protocol = DHCP

بروتوكول التشكيل الدينامي



يستخدم هذا البروتوكول لتوزيع عناوين **IP** بشكل اتوماتيكي لحواسب مضيفة **HOST** أو محطات عمل **Workstations** على شبكة **TCP / IP**، وبذلك نتجنب حالات التضارب في عناوين (**IP address conflict**) والتي تحدث نتيجة استخدام نفس عنوان **IP** لأكثر من جهاز على الشبكة (عند تركيب العناوين بشكل يدوي) مما يؤدي إلى فصل بعض الأجهزة عن الشبكة ،فهذا البروتوكول نظام لاكتشاف العناوين المستخدمة مسبقا.

يتألف **DHCP** من مكونين : بروتوكول لإرسال متغيرات التشكيل من المخدم إلى العميل وتقنية لتوزيع عناوين الشبكة على الحواسب المضيفة. وقد بني على نموذج مخدم - زبون (**Client-Server**)، فالحواسب المضيفة لا يجب أن تعمل كمخدمات **DHCP** إلا أن أعدت بشكل واضح للقيام بذلك من قبل مسؤول النظام **System Administrator** .

عندما ا تسند العناوين أو تغير فعلى الخادم **DHCP** أن يحدث المعلومات الموجودة على خادم **DNS** كما في **BOOT**، يستخدم **DHCP** العنوان الفيزيائي (**MAC**) في إسناد عناوين **IP** بني بروتوكول **DHCP** اعتمادا على **BOOTP** وحل محله.

- **تقنيات التوزيع : يدعم DHCP ثلاث تقنيات لتوزيع العناوين**

1-Static Configuration الإعدادات اليدوية

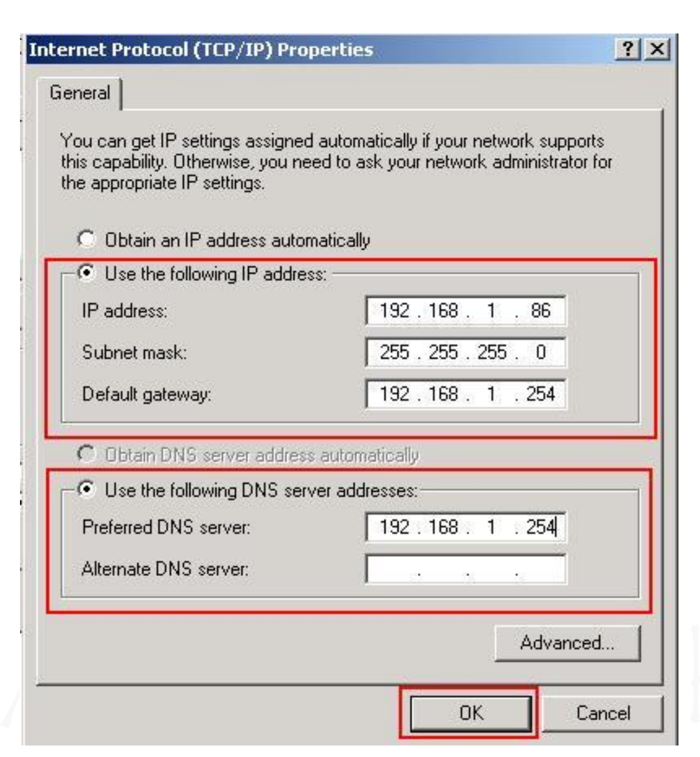
2-Dynamic Configuartion الإعدادات الديناميكية

3-Alternate Configuartion الإعدادات البديلة

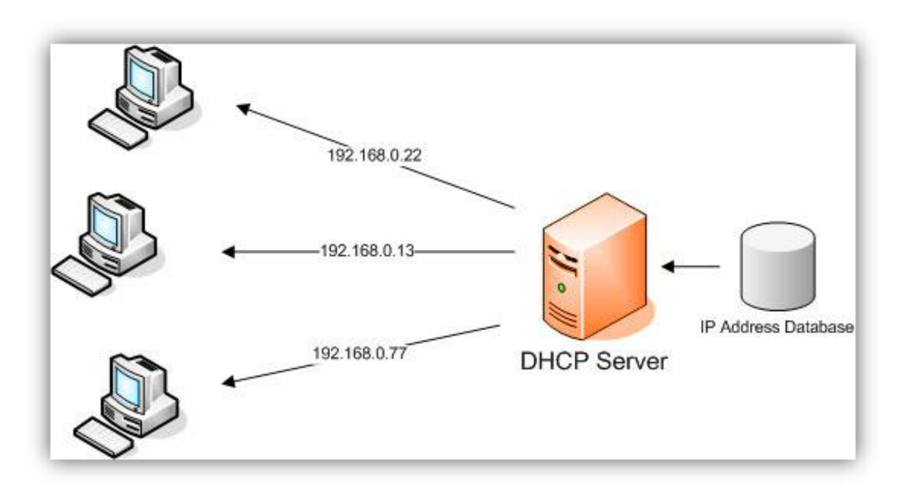
- **سأقوم بشرح هذه التقنيات بالتفصيل لنتعرف على كل واحد ماذا تفرق عن الآخر .**

- التوزيع الديناميكي هو الوحيد بين التقنيات الثلاث الذي يسمح بإعادة استخدام عنوان لم يعد مستخدما من قبل العميل الذي كان هذا العنوان قد أسند إليه، لذا فإن التوزيع الديناميكي مفيد بشكل خاص لإسناد العناوين لعميل يريد الاتصال بالشبكة بشكل مؤقت أو للتشارك بمجال محدد من عناوين **IP** لمجموعة من العملاء الذين لا يحتاجون إلى عنوان **IP** في شبكة معينة قد تستخدم واحدة أو أكثر من التقنيات السابقة وذلك اعتمادا على سياسة مسؤول الشبكة.

الإعدادات اليدوية Static Configuration : هي عبارة عن تركيب عنوان الاي بي بشكل يدوي من قبل مهندس الشبكة هو الذي يقوم بتركيب العناوين , و مثال على ذالك الخوادم التي هي السيرفرات هي تاخذ العناوين بشكل يدوي ولا ينصح أن تكون بشكل ديناميكي , لي إنه السيرفرات لا يجب أن تتغير العناوين الخاصة فيهم و يجب أن تكون ثابته ولا تتغير ابداً كما في الصورة التالية .

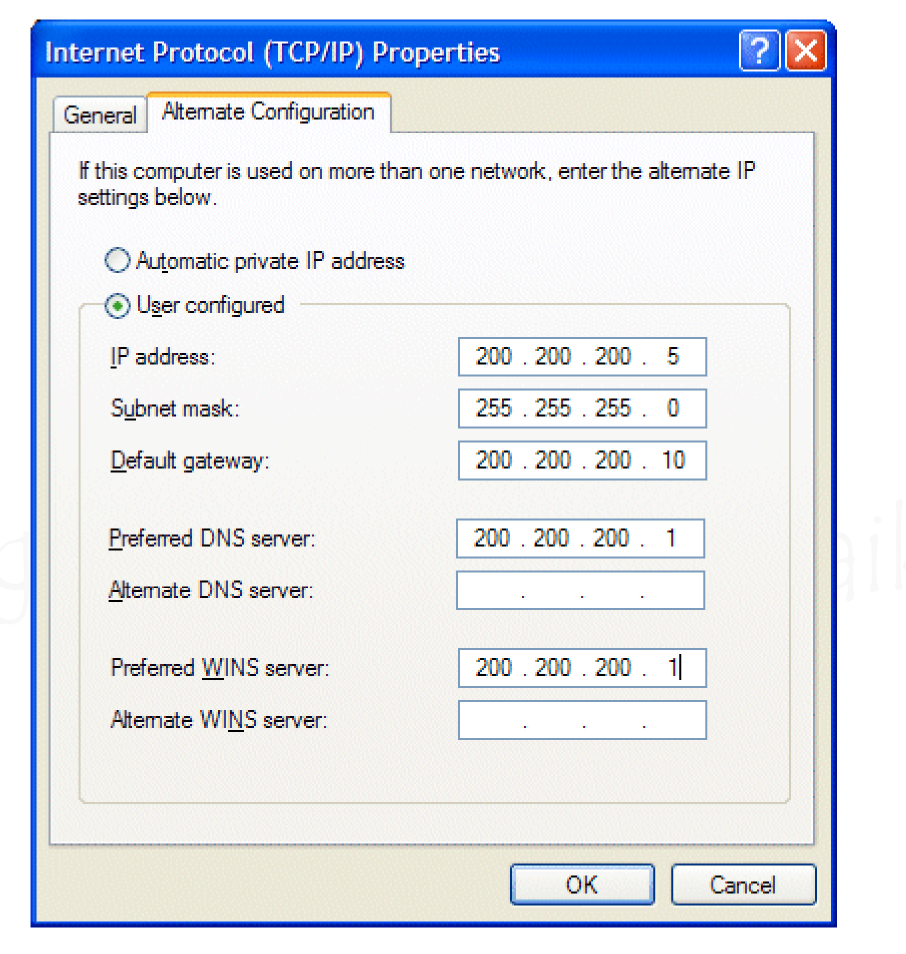


الإعدادات الديناميكية Dynamic Configuartion : هذه الطريقة الاتوماتيكية حيث يقوم مهندس الشبكة بعمل الإعدادات على سيرفر أو على جهاز راوتر لعمل خدمة الـ **DHCP** عليه ليقوم بتوزيع العناوين بشكل اتوماتيكي عن طريق هذا البروتوكول الـ **DHCP** وتكون هذه العملية من الطرفين من المضيف و من الخادم أو السيرفر , يبداء في عملية طلب عنوان الاي بي سيبدا أولاً المضيف بإرسال طالب لسيرفر الخدمة الـ **DHCP** ليقوم بتركيب الاي بي عليه تبداء هذه العملية عن طريق عدة خطوات يقوم فيه المضيف و الخادم سأقوم بذكر و شرح هذه الخطوات .



الإعدادات البديلة Alternate Configuartion : هذه المرحلة التي تكون بعد مرحلة الـ **Static** و **Dynamic** تاتي هذه الإعدادات في حال لم يجد المضيف عنوان اي بي يدوي ولا سيرفر يقوم برد عليه ليقوم باعطه عنوان اي بي , ياتي دور هذه الإعدادات البديلة **Alternate** يكون مركب فيه عنوان اي بي من قبل مهندس الشبكة ليعمل بيه الجهاز, وفي حال لم يجد الـ **Alternate** ايضاً سيتم تحويله للمرحلة الرابعة و هي مرحلة الـ**APIPA** و هي التي سبق أن شرحت عنها في الدروس السابقة .

الصورة التالية توضح إعدادات الـ Alternate Configuartion

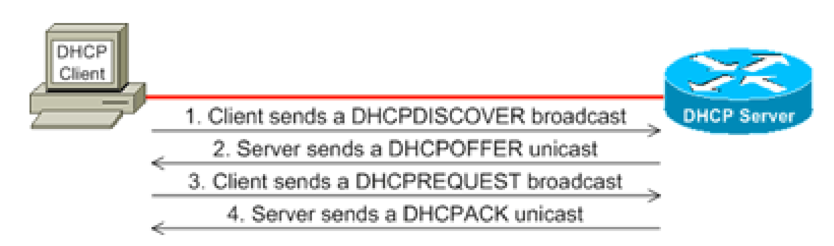


- الخدمات التي يتم توزيعها مع عنوان الاي بي من بروتوكول الـ **DHCP** يوجد عدة خدمات يتم توزيعها سأقوم بذكر ها :

1- IP Address
2- Subnet Mask
3- IP Default Gateway
4- DNS Server
5- WINS
6- Time

- **مراحل حصول المضيف على عنوان IP مؤجر (DHCP Lease Stages) من الخادم الذي يقوم بتوزيع العناوين .**

- عملية الحصول على عنوان **IP** تبداء باربع خطوات كما في الصورة التالية و سأقوم بشرح هذه الخطوات بالتفصيل :



- لاحظ إنه في الصورة يوضح كيفية الطلب و سأقوم بشرح هذه الخطوات بالتفصيل مع الامثلة لنستطيع فهم هذه الخطوات بشكل ممتاز .

1- Client Sends a DHCP Discover Broadcast
2- Server Sends a DHCP Offer Unicast
3- Clinet Sends a DHCP Request Broadcast
4- Server Sends a DHCP ACK Unicast

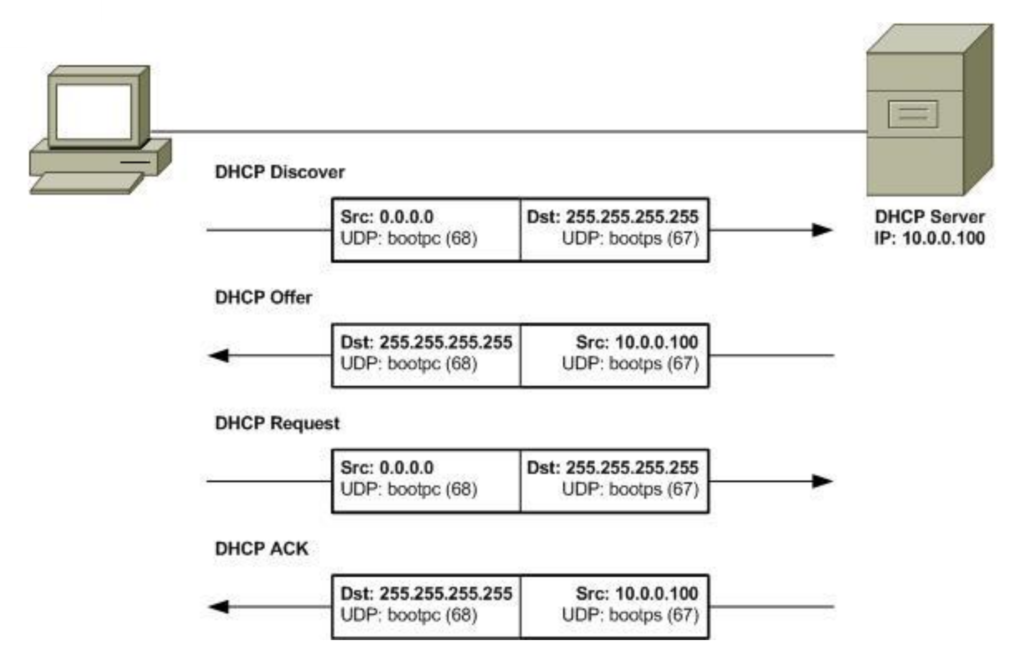
Client Sends a DHCP Discover Broadcast : هذه الرسالة سيتم إرسال عندما ا يبداء جهاز الحاسوب بطلب عنوان **IP** , سيقوم بإرسال هذه الرسالة الى السويتش المتصل فيه , و تحتوي هذه الرسالة على **Broadcast** البث المباشر يطلب في هذه الرسالة من لديه خدمة توزيع الـ **IP** , سيرد عليه الخادم أو جهاز الراوتر إذا كان مفعل عليه خدمة الـ **DHCP** يقول له انا اقوم بتوزيع عناوين **IP** , في هذه المرحلة سيتم إرسال رد للجهاز الذي قام بإرسال الطلب و هنا ياتي دور الطلب الثاني و هي الـ **Offer** سأقوم بشرحها لوحده تابع.

Server Sends a DHCP Offer Unicast: هذه الرسالة التي سيتم إرسال ه الى المضيف الذي قام بطلب عنوان **IP**، و تحتوي هذه الرسال على **Unicast** بمعنى إنه السيرفر لقد تمكن من معرفة المضيف الذي يريد عنوان **IP**، و الأن تم الرد عليه بهذه الرسالة ليقوم المضيف بمعرفة إنه يوجد سيرفر يقوم بتقديم خدمة **DHCP** و سيتم الانتقال للمرحلة الثالثة تابع.

Clinet Sends a DHCP Request Broadcast : ياتي دور هذه الرسالة بعد أن تم التعرف على سيرفر الخدمة **DHCP** ، الأن في هذه الرسالة سيقوم المضيف بإرسال ه للسيرفر يطلب فيه عنوان **IP** سيقوم سيرفر الخدمة الـ **DHCP** بحجز عنوان الـ **IP** للجهاز الذي يريد هذا العنوان ، و طريقة الحجز تتم عن طريق الماك ادرس الخاص في الجهاز الذي اخذ هذا العنوان الـ **IP** , و سيقوم بإرسال ه للجهاز بهذه الحالة المضيف قد حصل على عنوان **IP** و تبقى رسالة واحد و هي رسالة التاكيد على استلام عنوان الـ **IP**.

Server Sends a DHCP ACK Unicast: هذه رسالة التاكيد على استلام عنوان الـ **IP** , و هذه الرسالة يقوم بإرسال ه سيرفر الخدمة **DHCP** ليأكيد على استلام العنوان .

هذا النموذج يوضح عملية الطلب و تمسى هذه العملية DHCP DORA



بروتوكول الـ **DHCP** يعمل مع بروتوكول الـ **UDP** ويعمل على بورتين سأقوم بذكرهم:

DHCP Server يعمل ببروتوكول الـ **UDP Port 67** .

DHCP Client يعمل ببروتوكول الـ **UDP Port 68** .

تجديد ايجار DHCP: بعد انقضاء **50%** من مدة الإيجار يحأول الزبون تجديد (**renew**) الإيجار من خادم الـ **DHCP** الأصلي الذي أجره عنوان **IP** يستمر الزبون بمحأولة التجديد هذه وعند إكمال **87.5%** من مدة الإيجار يحأول الزبون الاتصال بأي خادم **DHCP** للحصول على ايجار جديد إن انتهت مدة الإيجار يرسل الزبون **DHCP DISCOVER** من جديد طالبا الحصول على عنوان **IP** فهو لم يعد يملك عنوانا.

DHCP Relay Agents: هذه خدمة الـ **DHCP** يدعم الشبكات التي تكون فرعية مثل عندما ا يتواجد راوتر في المنتصف يربط ما بين شبكة المستخدمين و شبكة السيرفرات ، و نريد توزيع عناوين من سيرفر خدمة الـ **DHCP** على شبكة المستخدمين ولكن في هذه الحالة لان يستطيع اي مستخدم من طلب اي عنوان من سيرفر الخدمة الـ **DHCP** لي لأنه يوجد في المنتصف جهاز راوتر و كما نعرف إنه جهاز الراوتر يمنع البث المباشر الـ **Broadcast** ، في هذه الحالة الان يستطيعوا الاتصال في سيرفر الخدمة الـ **DHCP** ولكن تم حل هذه المشكلة عن طريق خدمة الـ **DHCP Relay Agents** و هي عبارة عن خدمة نقوم بتفعيلها على الراوتر الذي يربط الشبكات في بعضها البعض ليستطيع المستخدمين من العبور على شبكة السيرفرات و الاتصال في سيرفر الخدمة الـ **DHCP** بهذه الطريقة نكون قد فهمنا ماذا تفعل خدمة الـ **DHCP Relay Agents** ولكن لن اقوم بشرح هذه الخدمة بشكل تطبيقي و عملي لي لأنه من المستوى الاعلى من هذه الدروس و هي من مستوى المحترفين سنتعرف عليه بشكل اكبر في دروس المحترفين .

حجز المضيف في سيرفر الخدمة الـ Client Reservation DHCP : تستخدم هذه الطريقة للتأكد من أن الحاسب يأخذ نفس عنوان **IP** كل الوقت، لذا بعد اسناد عنوان **IP** من قبل خادم الـ **DHCP** اعتمادا على العنوان الفيزيائي للزبون العنوان الفيزيائي **MAC Address** فإن التالي مطلوب لحجز الزبون:

١- العنوان الفيزيائي **MAC** ٢- عنوان **IP**

إعدادات بروتوكول الـ DHCP

DHCP Configuration

Router > **enable**

Router # **config t**

Router (config) # **ip dhcp excuded-address 10.0.0.1 10.0.0.50**

Excuded-address هذا الأمر نقوم بتفعيله عندما ا نريد حجز عناوين محددة وعدم توزيع هذه العناوين في الشبكة الا عن طريق مهندس الشبكة.

Router (config) # **ip dhcp pool HR** ← اسم القسم الذي سيتم توزيع العناوين منه

Router (dhcp-config) # **network 10.0.0.0 255.0.0.0**

Router (dhcp-config) # **default-router 10.0.0.100**

Router (dhcp-config) # **dns-server 10.0.0.99**

Router (dhcp-config) # **end**

Router # **show ip dhcp binding**

هذا الأمر لعرض العناوين التي تم توزيعها

- الأن سنقوم بتطبيق عملي و نقوم بتفعيل خدمة الـ **DHCP Server** على جهاز راوتر سنقوم بتطبيق على نموذج مكون من عدة أجهزة حاسوب و ننظر كيف سيتم طلب عنوان و اخذه من الـ **DHCP Server** الأن سنقوم بتعرف على إعدادات الشبكات التي سنقوم بتطبيق عليها .

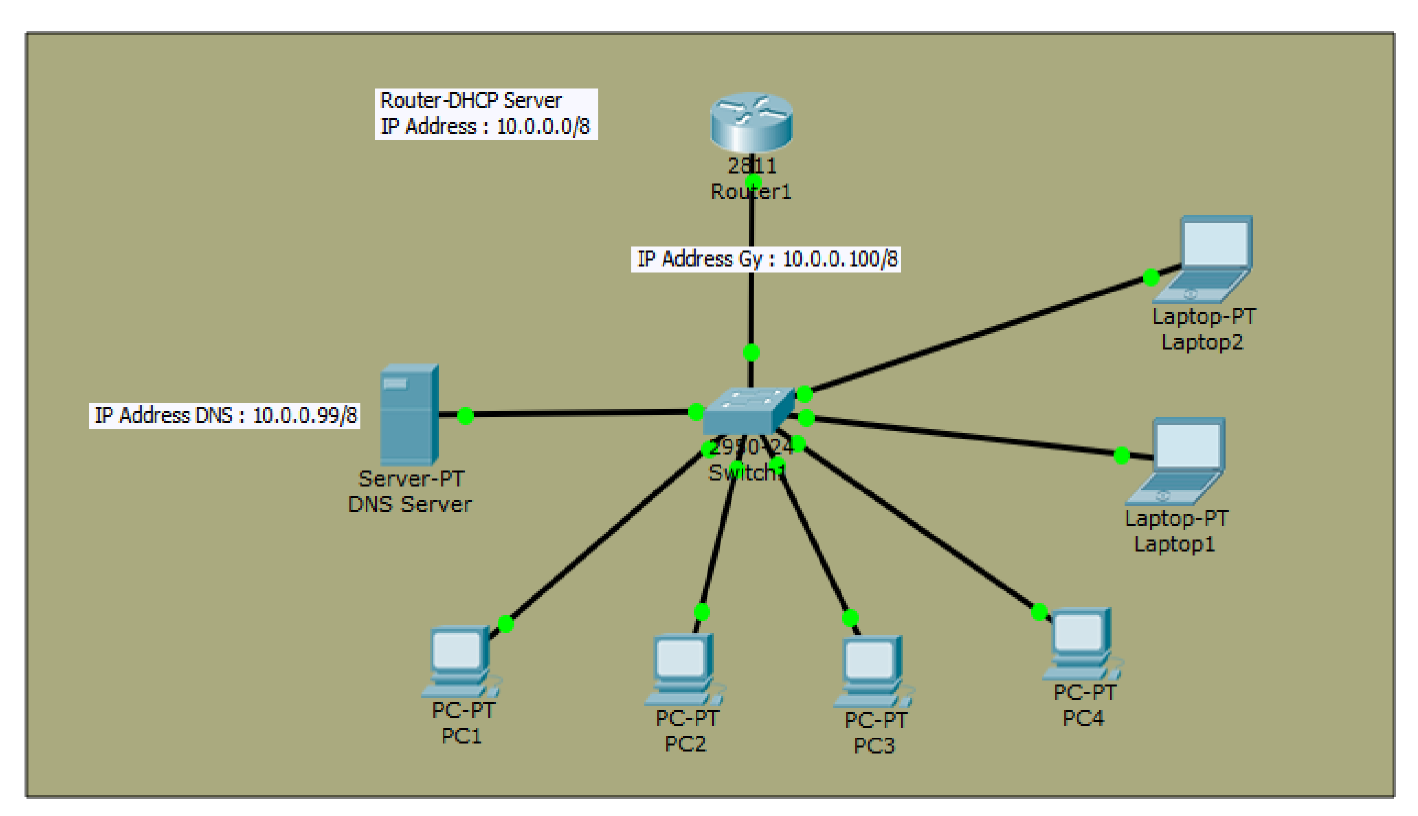
- إعدادات الشبكة سنقوم بتعرف على إعدادات الشبكة قبل أن نبداء بعملية التطبيق .

١- سنقوم بتفعيل خدمة الـ **DHCP Server** على جهاز الراوتر .

٢- سيكون نطاق العناوين من الفائة **A** بمعنى سيبدا توزيع العناوين من نطاق الـ **10.0.0.0/8** .

٣- سيكون لدينا سيرفر **DNS** و يمتلك عنوان **IP 10.0.0.99/8**.
٤- عنوان الـ **IP** لجهاز الراوتر الذي سيكون من الطبيعي هو الـ **GY : 10.0.0.100/8** .
٥- سنقوم بدخول على بعض أجهز الحاسوب الموجودة لنرى هل تم سحب عنوان **IP** من سيرفر الخدمة الـ **DHCP Server** أو لا .

النموذج الذي سنقوم بتطبيق عليها



- **الأن سنقوم بدخول على جهاز الراوتر لنقوم بعمل الإعدادات التالية :**

سنقوم بكتابة الاوامر التالية :

Router > **enable**

Router # **config t**

Router (config) # **interface fastethernet 0/0**

Router (config-if) # **ip address 10.0.0.100 255.0.0.0**

Router (config-if) # **no shutdown**

Router (config-if) # **exit**

Router (config) # **ip dhcp pool HR**

Router (dhcp-config) # **network 10.0.0.1 255.0.0.0**

Router (dhcp-config) # **default-router 10.0.0.100**

Router (dhcp-config) # **dns-server 10.0.0.99**

Router (dhcp-config) # **end**

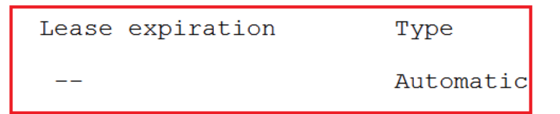
Router # **copy running-config startup-config**

كما في الصورة التالية من داخل الراوتر :

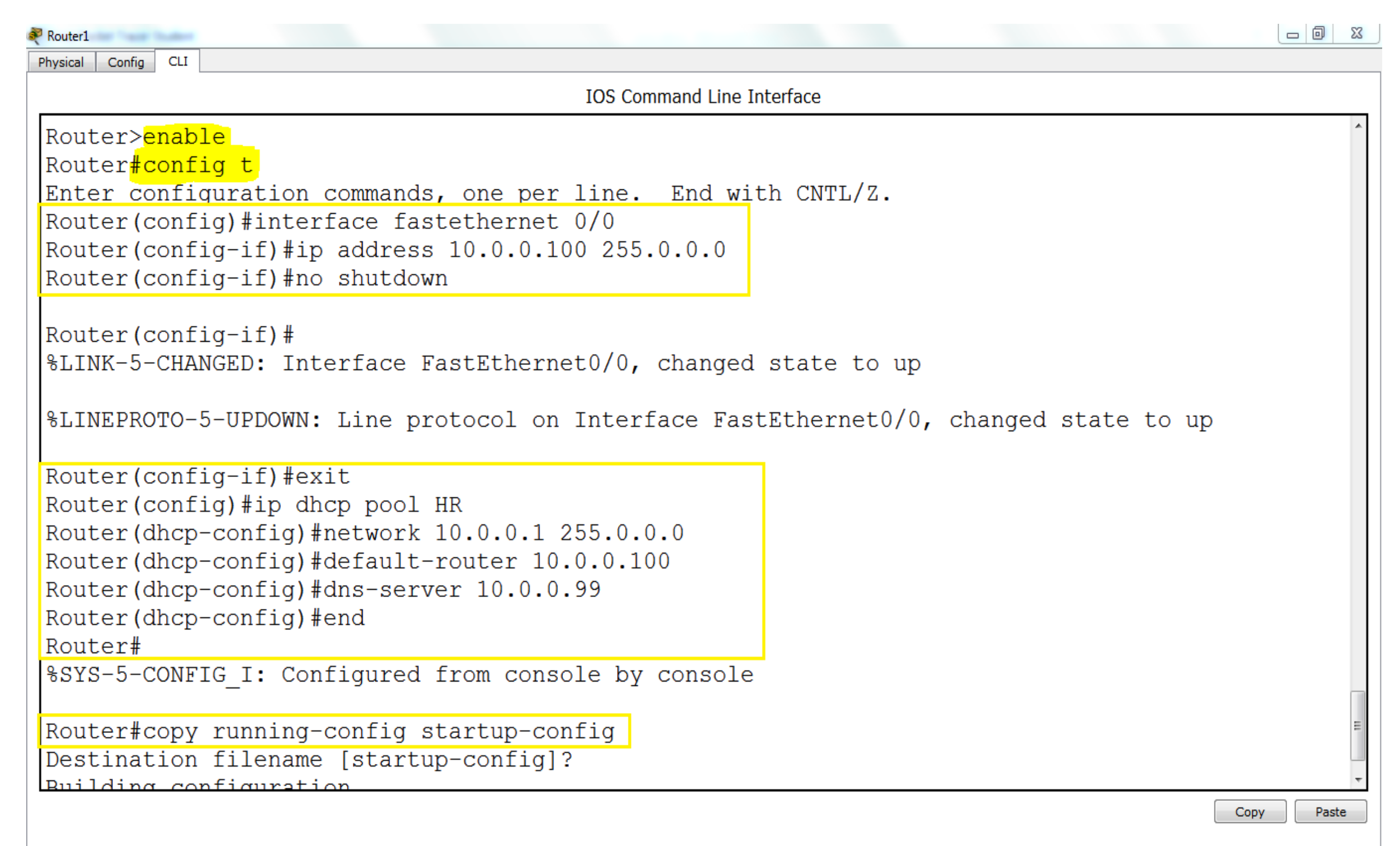
- بهذه الإعدادات نكون قد قمنا بتفعيل خدمة الـ **DHCP Server** على جهاز الراوتر و الأن نريد أن نقوم بعرض العناوين التي تم توزيعها على الأجهزة التي في الشبكة سنقوم بكتابة الأمر التالي لعرض العناوين .

Router # **show ip dhcp binding**

```
Router#show ip dhcp binding
IP address        Client-ID/
                  Hardware address
10.0.0.1          0001.C774.16D6
Router#
```



```
Lease expiration          Type
 --                       Automatic
```



Router1

Physical | Config | CLI

IOS Command Line Interface

```
Router>enable
Router#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#interface fastethernet 0/0
Router(config-if)#ip address 10.0.0.100 255.0.0.0
Router(config-if)#no shutdown

Router(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up

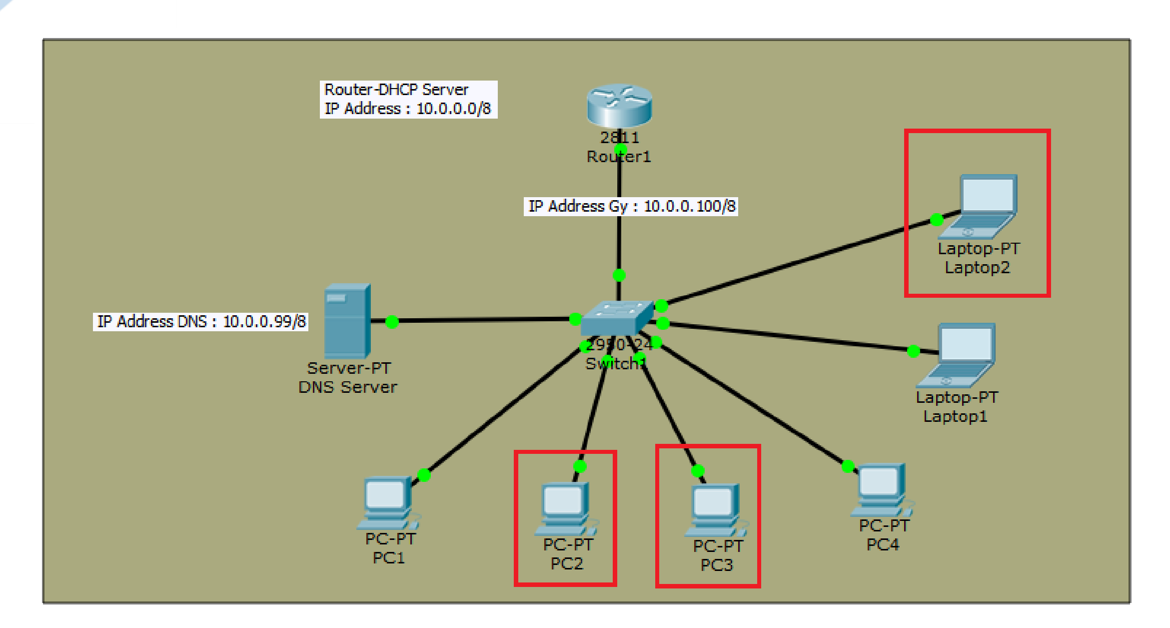
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up

Router(config-if)#exit
Router(config)#ip dhcp pool HR
Router(dhcp-config)#network 10.0.0.1 255.0.0.0
Router(dhcp-config)#default-router 10.0.0.100
Router(dhcp-config)#dns-server 10.0.0.99
Router(dhcp-config)#end
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
```

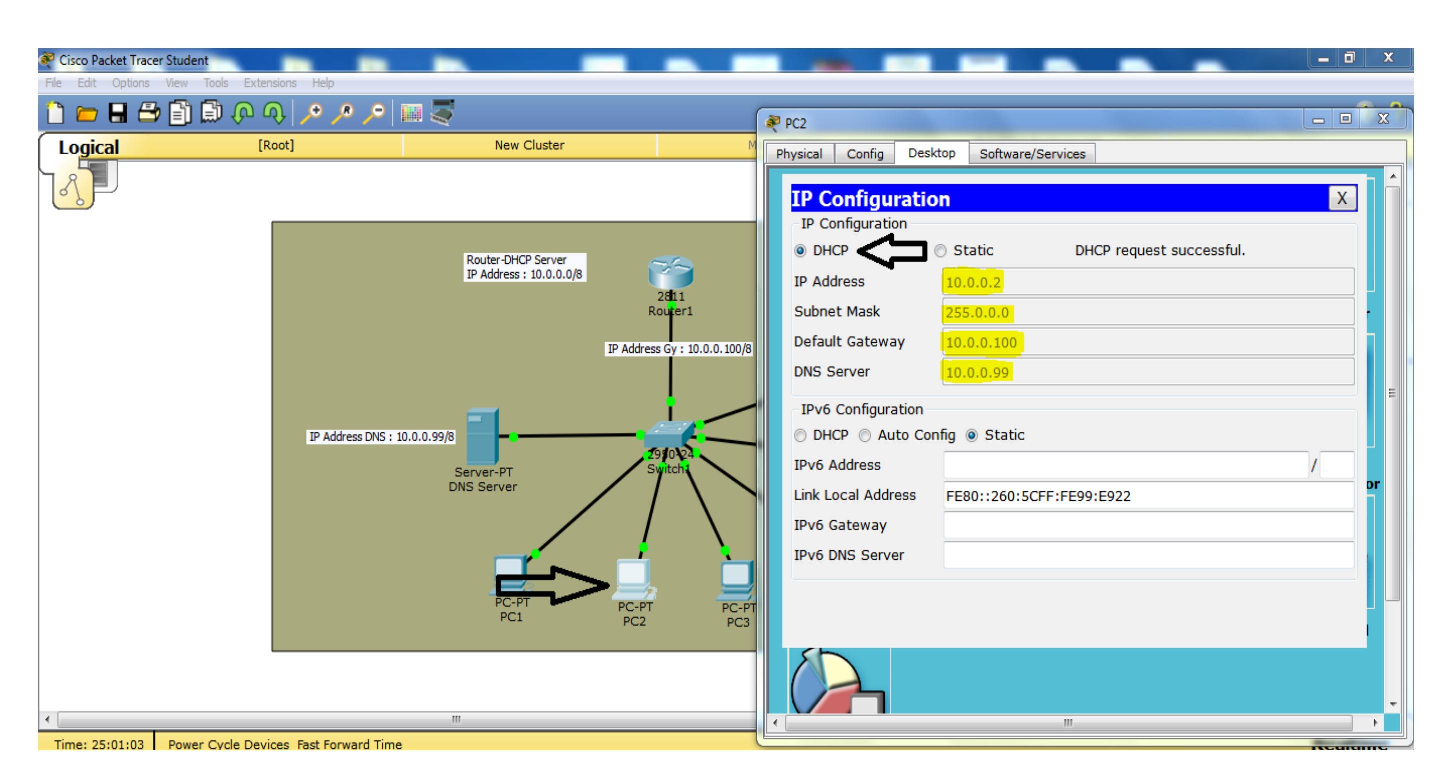
Copy | Paste

- لاحظ إنه تم توزيع عنوان **IP** واحد فقط و هو العنوان **10.0.0.1** و هذا العنوان تم اخذه من قبل جهاز حاسوب في داخل الشبكة و يساوي هذا العنوان ، عنوان الماك ادرس الخاص في جهاز الحاسوب و لاحظ ايضاً إنه لا يوجد عملية توقيت للعنوان .
- الأن سنقوم بدخول على أحد أجهزة الحاسوب في الشبكة و نفرض عليه أن ياخذ عنوان **IP** من سيرفر الخدمة الـ **DHCP Server** نتابع النموذج التالي .



- سنقوم الأن بدخول على هذه الأجهزة و نفرض عليها أن تقوم بسحب عنوان **IP** من سيرفر الخدمة **DHCP Server** تابع التالي :
- لاحظ بعد الدخول لجهاز الحاسوب المسمى **PC 2** قمنا بتغير الاختيار الذي كان **Static** بمعنى الاختيار اليدوي الى اختيار الـ **DHCP**، وبعد الاختيار لاحظ إنه تم سحب عنوان **IP** بعنوان **10.0.0.2**، و باقي الخدمات الآخر مثل قناع الشبكة و البوابة و سيرفر الـ **DNS** جميع الإعدادات التي قمنا بتفعيلها على جهاز الراوتر .

- وسنقوم بنفس الطريقة على باقي الأجهزة الموجودة على الشبكة لتقوم جميع الأجهزة بسحب العناوين ، الأن سنقوم بدخول على جهاز الراوتر مره اخرى و نقوم بعرض العناوين التي تم سحبها من سيرفر الخدمة الـ **DHCP** سنقوم بكتابة الأمر التالي :



Router # **show ip dhcp binding**

```
Router#show ip dhcp binding
IP address       Client-ID/              Lease expiration        Type
                 Hardware address
10.0.0.1         0001.C774.16D6           --                     Automatic
10.0.0.2         0060.5C99.E922           --                     Automatic
10.0.0.3         0060.70E0.A2DE           --                     Automatic
10.0.0.4         0005.5EA9.42C6           --                     Automatic
10.0.0.5         0001.C940.A086           --                     Automatic
10.0.0.6         0002.1747.1246           --                     Automatic
Router#
```

- لاحظ إنه تم سحب اكثر من عنوان **IP** على عدد الأجهزة الموجودة على الشبكة ، بهذا الشكل يكون قد تم الانتهاء من إعدادات خدمة الـ **DHCP** على جهاز الراوتر و الأن سنقوم بتعرف على طريقة إعدادات خدمة الـ **DHCP** على السيرفر نتابع التالي الدرس التالي .
- في هذه الدرس سنقوم بتطبيق على نموذج مكون من سيرفر **DHCP** و يخدم على شبكتان ، كما في النموذج التالي :
- الأن سنقوم بتعرف على إعدادات الشبكة التي في النموذج لنقوم بعمل إعدادات لسيرفر الخدمة الخاص في الـ **DHCP** الإعدادات كتالي :

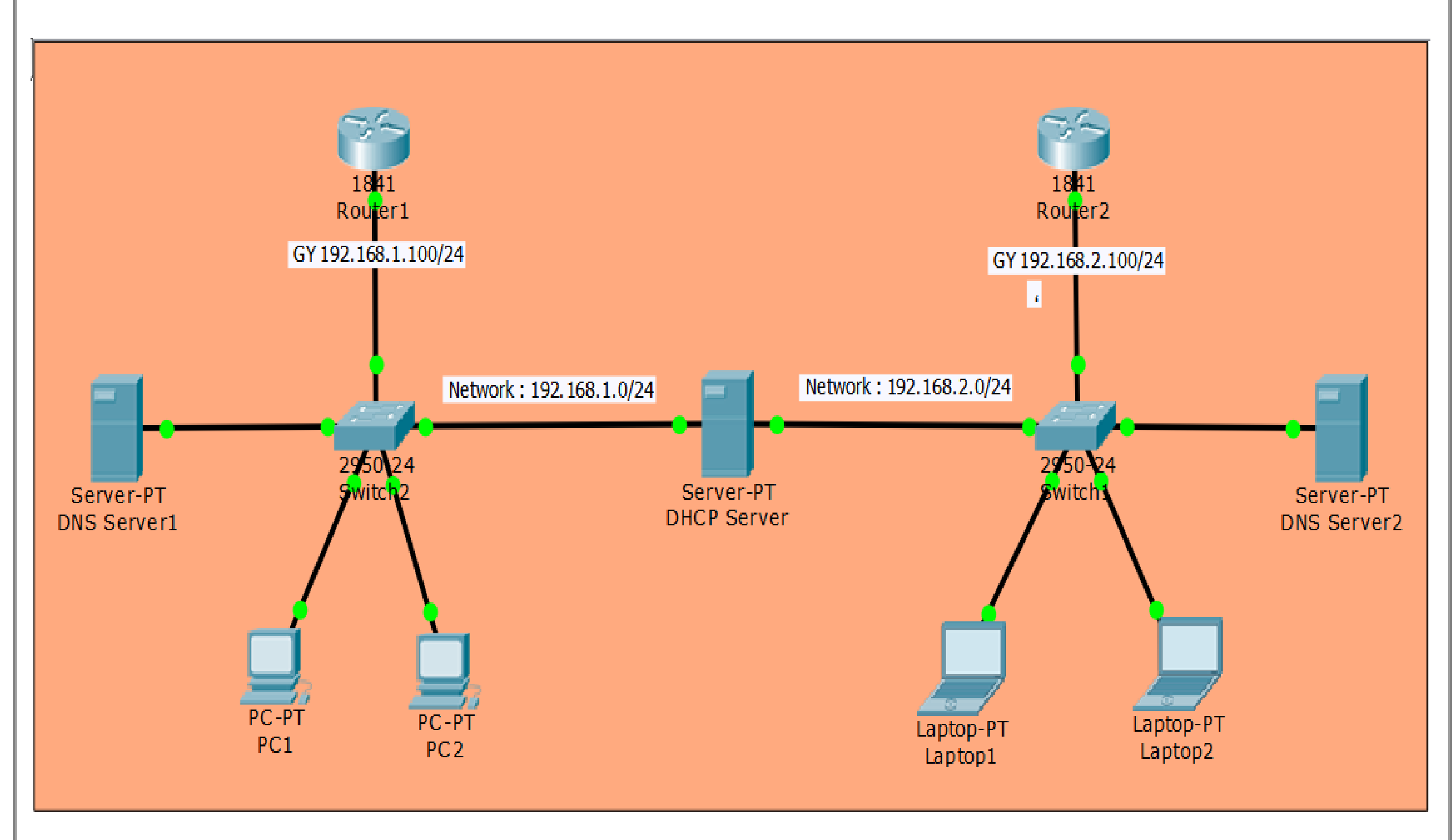
١- **سيتم بناء سيرفر الخدمة الـ DHCP و نقوم بتركيب كرتان شبكة عليه لنقوم بتوزيع العناوين على الشبكتين مختلفة العناوين .**

٢- الشبكة الأول ستكون بعنوان **IP 192.168.1.0/24.**

٣- الشبكة الثانية ستكون بعنوان **IP 192.168.2.0/24 .**

٤- يوجد في كل شبكة جهاز راوتر واحد و سيرفر **DNS** لنقوم بعملية التطبيق عليهم.

٥- سنقوم بجعل المضيف يقوم بسحب عنوان الـ **IP** من السيرفر كما سنرى .

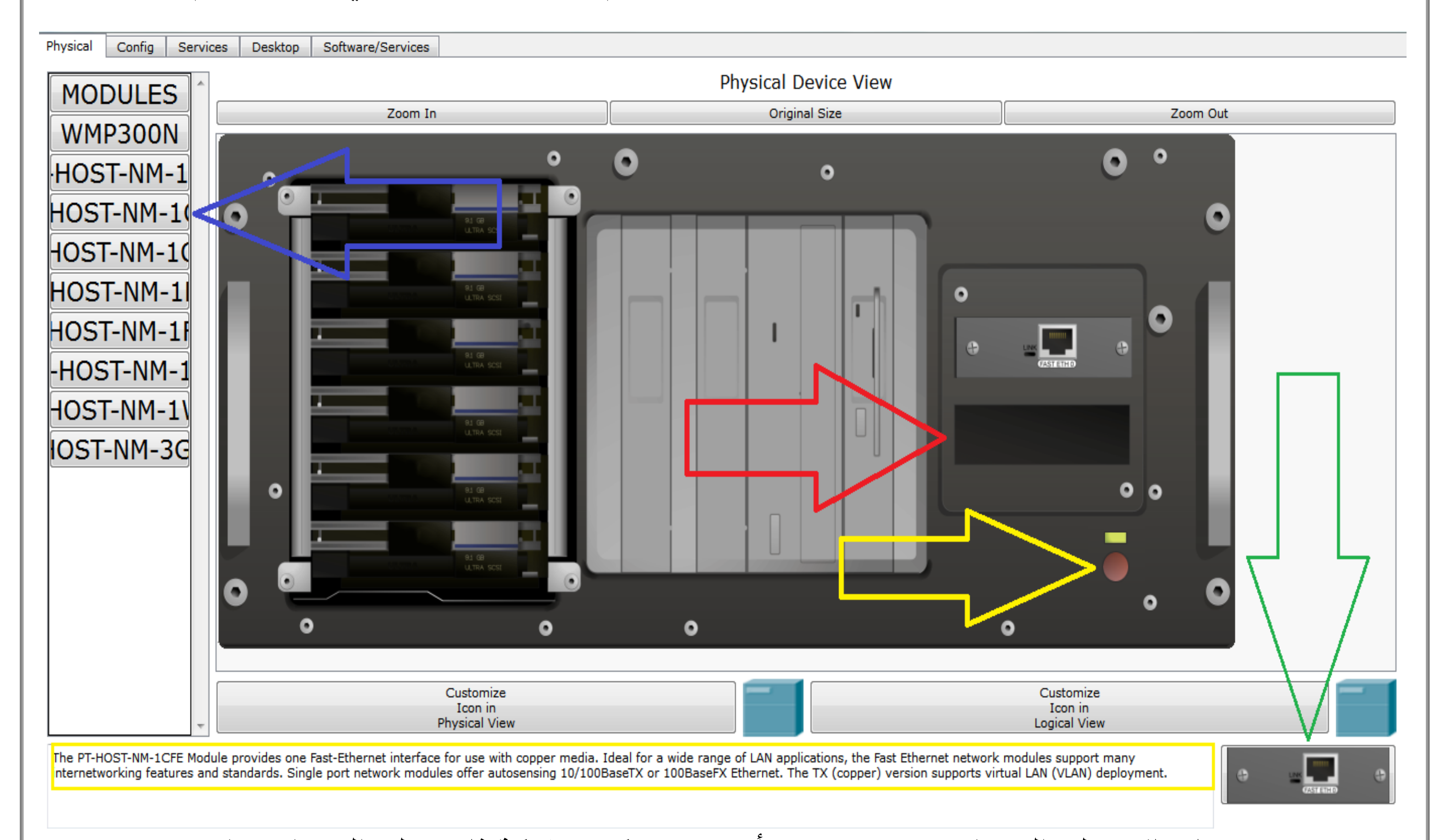


- الأن بعد أن تعرفنا على تصميم النموذج سنقوم بدخول للعملي و سنقوم بدخول على سيرفر الـ **DHCP** و نقوم بإضافة كرت شبكة اخرى كما في الصورة التالية :

DHCP Server

- الأن كما هو واضح بصورة سنقوم بتتبع الاسهم و سأقوم بشرح كل واحد من هذه الاسهم على ماذا تشير :

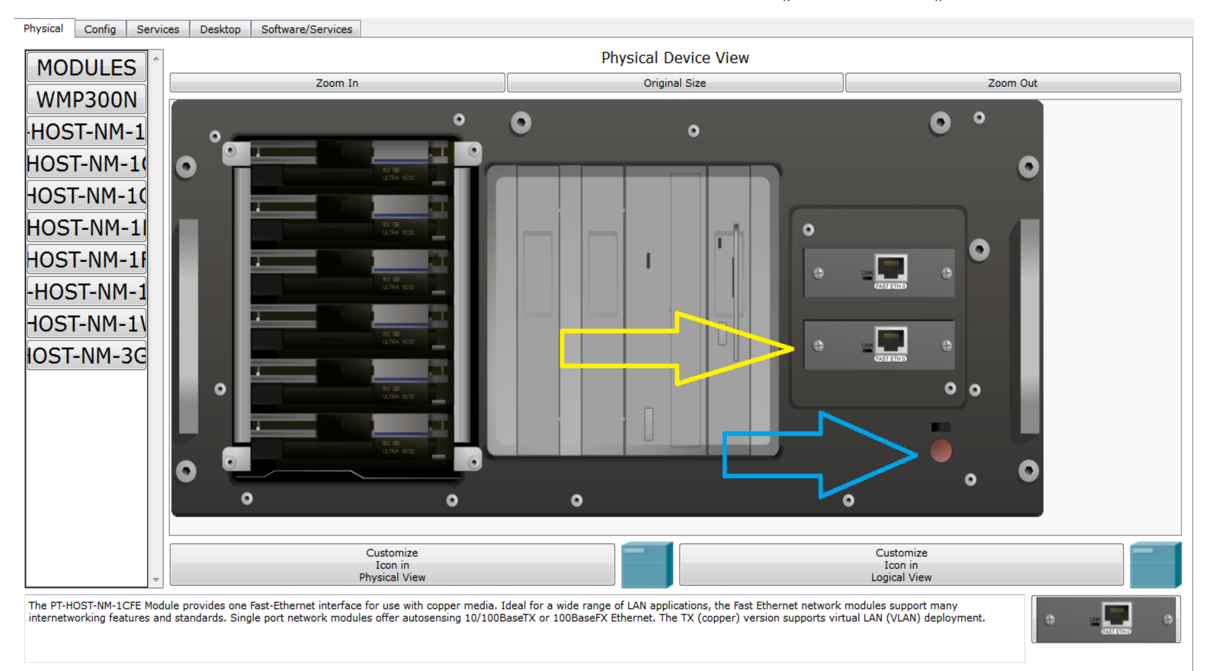
- قبل أن نقوم بإضافة اية إضافة من المكونات يجب أن نقوم باطفاء السيرفر ليتم إضافة المكونات , و هنا ياتي دور السهم الاصفر الذي يشير الى مفتاح ايقاف و تشغيل السيرفر ولكن في هذه الحالة نرى أن المفتاح مضيء هذا يعني إنه السيرفر قيد التشغيل , و نحن سنقوم بعملية ايقاف السيرفر بنقرة واحدة فقط على المفتاح الذي يشير اليه السهم الاصفر.
- الأن بعد أن قمنا بعملية ايقاف تشغيل السيرفر سنقوم باختيار المكونات التي نريدها لنقوم



باضافته على السيرفر , و نحن نريد أن نضيف كرت شبكة ثاني على السيرفر سنقوم بختير الكرت عن طريق الاسم الذي يشير اليه السهم الازرق من جهة اليسار و سنقوم باختير نوع الكرت المسمى **Host-NM-10/100** و هذا الكرت من نوع الايثرنيت , و قمت بتحديد المعلومات الخاصة في هذه النوع أنظر لي اسفل الصورة ستجد مربع محدد باللون الاصفر هذه المعلومات الخاصة في كرت الشبكة , و من الجانب الايمن يوجد سهم اخضر و منفذ ايثرنيت هذا هو الكرت الذي سنقوم باضافته على السيرفر

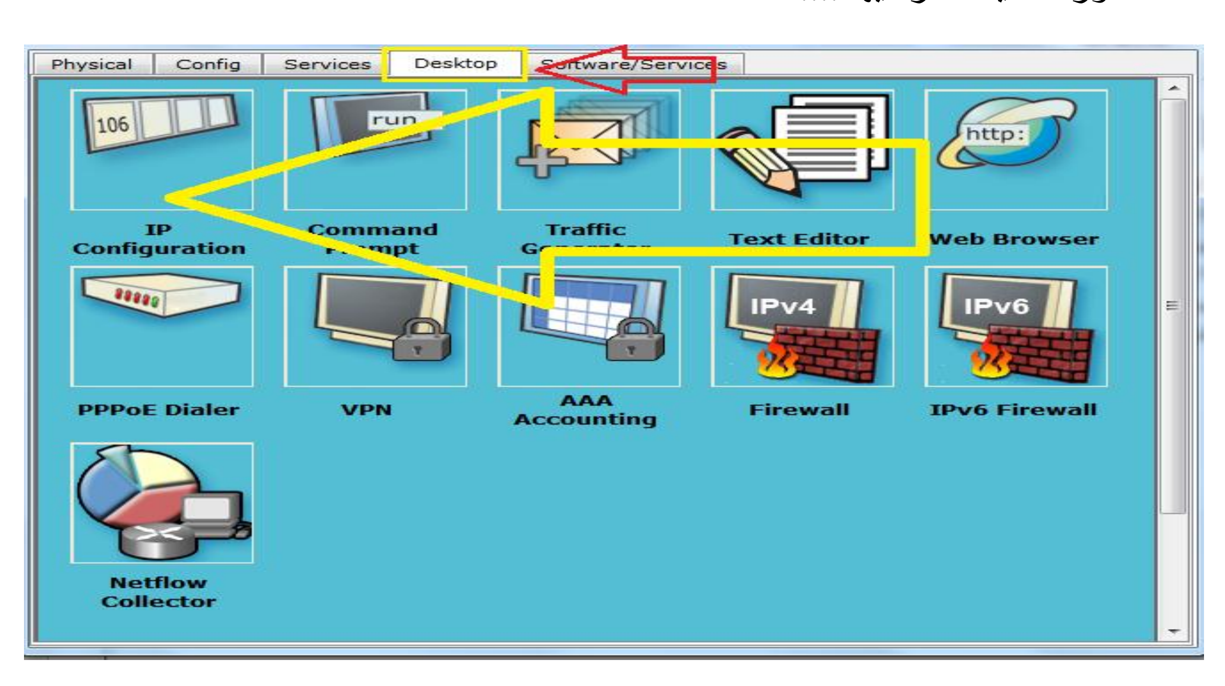
سنقوم فقط سحب هذا المنفذ و اضافته في المكان الفارغ الذي يشير اليه اسهم الاحمر , و بعد أن قمنا بإضافة الكرت سنقوم بتشغيل السيرفر كما في الصورة التالية ....

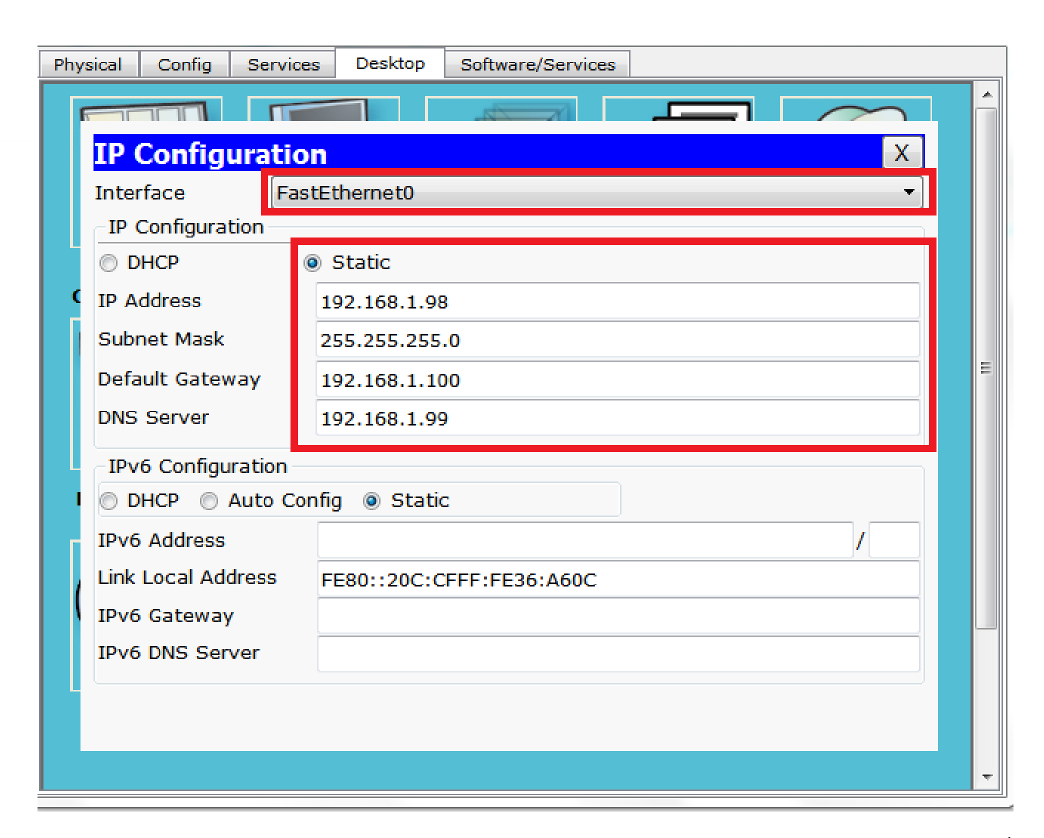
- كما نلاحظ في الصورة تم إضافة كرت شبكة ثاني على السيرفر الذي يشير اليه اسهم الاصفر , اما السهم الازرق هذا يشير على إنه مفتاح التشغيل مقفل يجب أن نقوم بتشغيلها ليبداء في السيرفر في العمل .



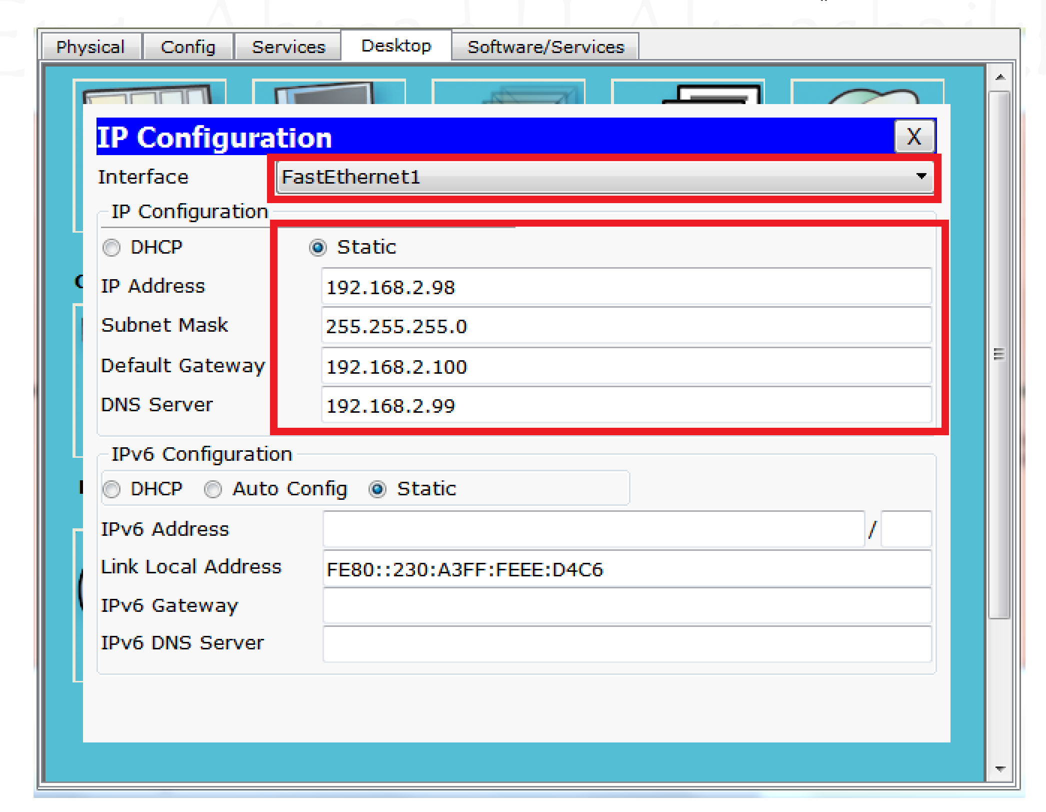
- الأن سنقوم بدخول على الإعدادات و تركيب العناوين على كروت السيرفر و سنقوم بدخول على إعدادات خدمة الـ **DHCP** لنقوم بتفعيلها و ترتيب بداية العناوين التي سيتم توزيعها على المضيفين في الشبكة تابع الصورة التالية :

- كما هو موضح في الصورة السابقة سنقوم بدخول على إعدادات المنفذ و نقوم بتركيب عنوان الـ **IP** على كرت الشبكة **Fast Ethernet 0/0** , كما هو موجود في الصورة التالية أنظر اليها ....

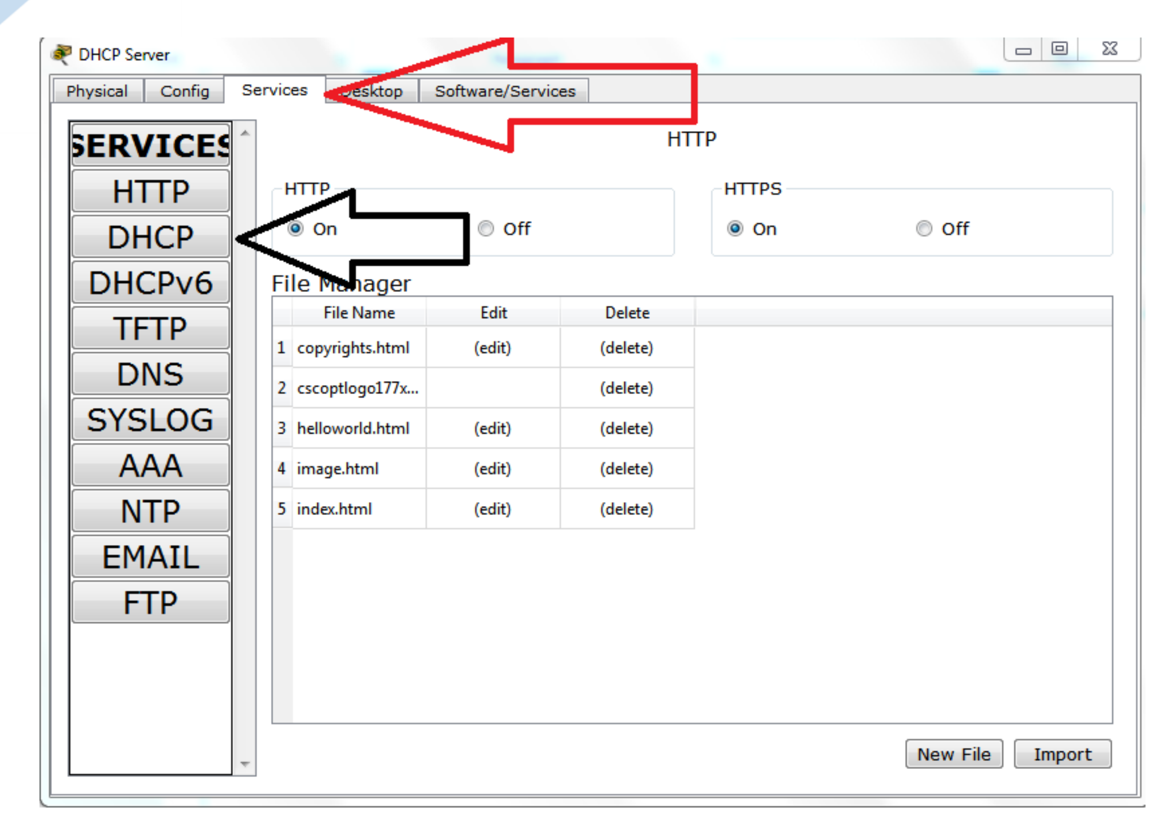




- الأن سنقوم بتركيب عنوان الـ **IP** على كرت الشبكة الثاني **Fast Ethernet 0/1** , كما هو موجود في الصورة التالية ......



- بهذه الطريقة نكون قد قمنا بتركيب العناوين سنقوم الأن بعمل الإعدادات الخاصة في خدمة الـ **DHCP** كما في الصورة التالية ....



- سنقوم بدخول على الـ **Services** و من داخل الخدمات سنقوم بدخول على الـ **DHCP** كما في الصورة التالية من داخل الخدمة سنقوم بعمل الإعدادات التالية :
- كما نلاحظ في الصورة سنقوم بكتابة اسم الـ **Pool Name** و هذه هي المجموعة التي سيكون فيها العناوين الـ **IP** , و بعدها الـ **Gy** عنوان الراوتر و بعده سيرفر الـ

DHCP Server

Physical | Config | Services | Desktop | Software/Services

SERVICES: HTTP, DHCP, DHCPv6, TFTP, DNS, SYSLOG, AAA, NTP, EMAIL, FTP

DHCP

Interface: FastEthernet0 — Service: On / Off

Pool Name: IT

Default Gateway: 192.168.1.100

DNS Server: 192.168.1.99

Start IP Address : 192 168 1 1

Subnet Mask: 255 255 255 0

Maximum number of Users : 255

TFTP Server: 0.0.0.0

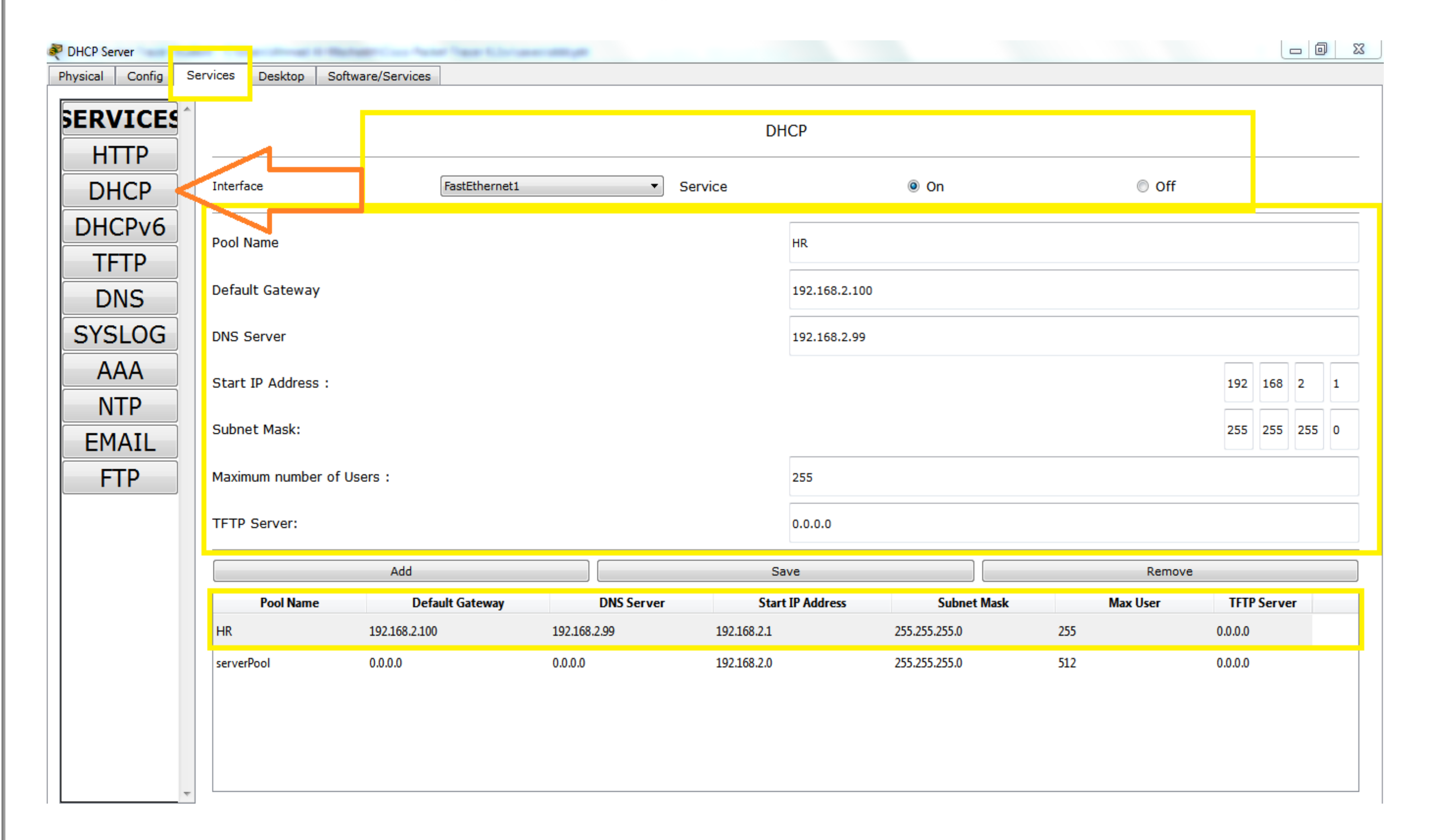
Add | Save | Remove

Pool Name	Default Gateway	DNS Server	Start IP Address	Subnet Mask	Max User	TFTP Server
IT	192.168.1.100	192.168.1.99	192.168.1.1	255.255.255.0	255	0.0.0.0
serverPool	0.0.0.0	0.0.0.0	192.168.1.0	255.255.255.0	255	0.0.0.0

DNS و بعده سيتم كتابة العنوان الذي سيبداء في توزيعها في داخل الشبكة الـ **Start IP Address** و قناع الشبكة الـ **SubnetMask** بهذا الشكل نكون قد اتمينا عملية الإعدادات و يتبقى لدينا خطوة واحد و هي عملية الإضافة **Add** .

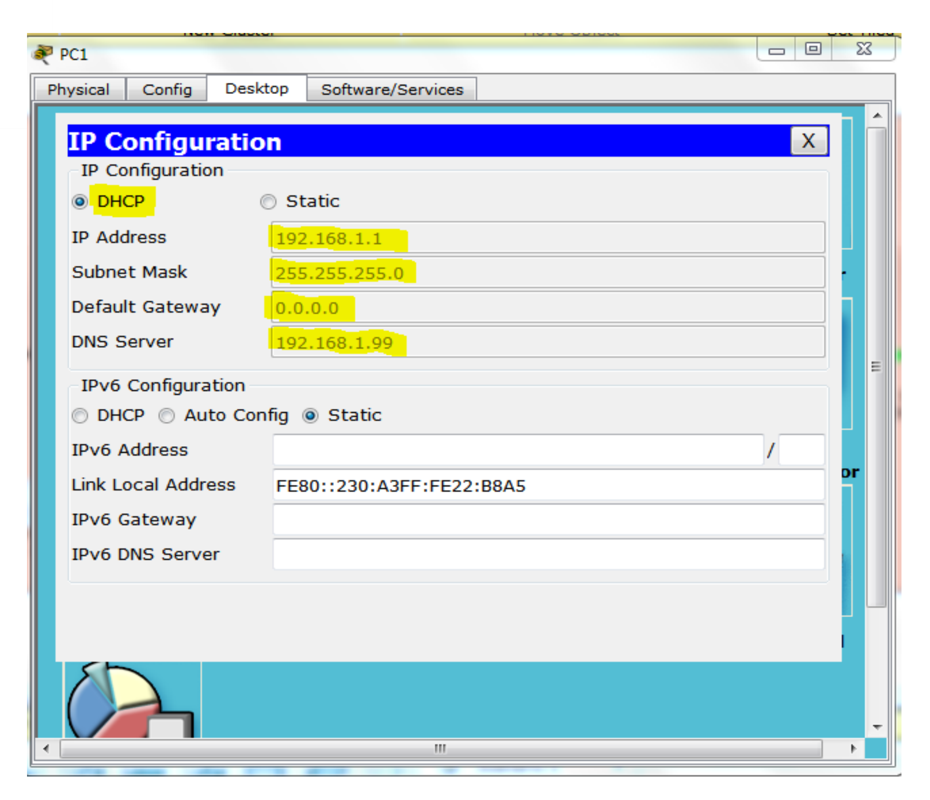
- **ملاحظة مهم جداً :** في هذه الحالة يكون تكون خدمة الـ **DHCP** معطلها و يجب أن نقوم بتشغيلها بمعنى من **Off** الى **ON**.
- ويجب أن نكون على معرفة بنفس هذه الإعدادات سنقوم بها على الكرت الثاني ولكن على مختلف العنوان أنظر للصورة التالية ......

- كما نلاحظ بهذه الإعدادات قمنا بتفعيل خدمة الـ **DHCP** على السيرفر و الأن اذا السيرفر يقوم بتقديم خدمة العناوين بشكل تلقائي لكل المضفين في الشبكة الأولى و الثانية.

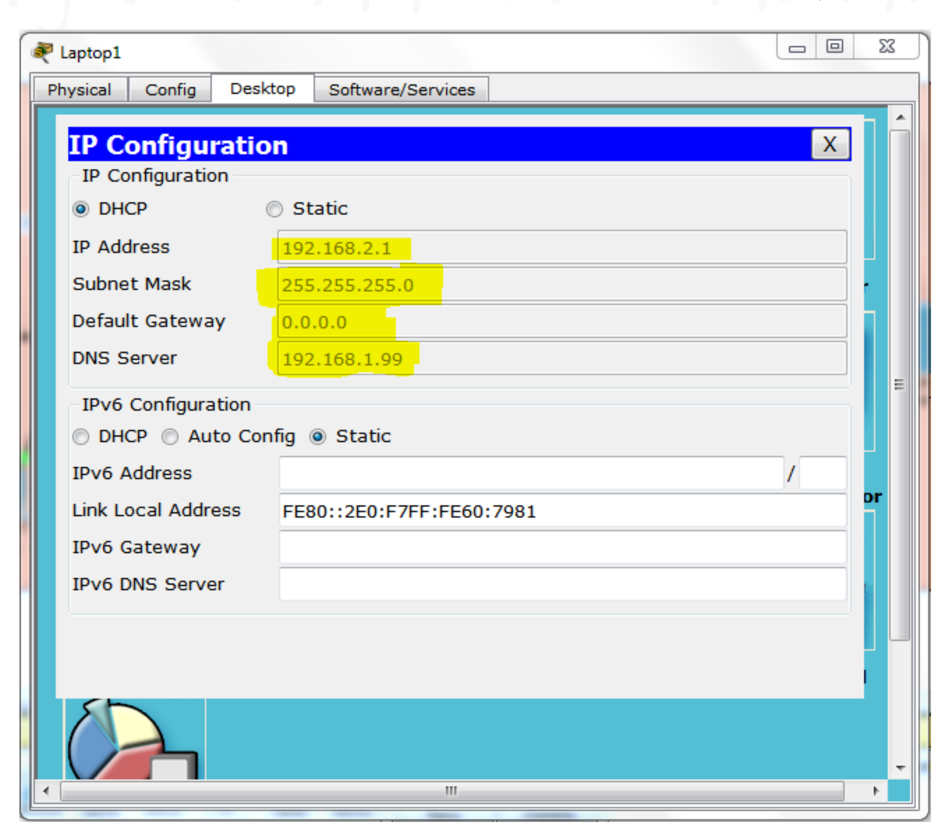


- **ملاحظة مهم جداً** : يجب أن تقوم بعدادات الراوتر انتا بنفسك ولان اقوم بعمل إعدادات لجهاز الراوتر يجب أن تعتمد على نفسك بعمل الإعدادات , لي لأنه قمنا بشرح هذه الإعدادات مسبقاً عدة مرات ويجب أن تكون في هذه المرحلة قد فهمت كيفية عملية الإعدادات و الاعتماد على نفسك .

- الأن سنقوم بدخول على أحد أجهزة المضيف في الشبكتين لنتاكد هل تم سحب عناوين الـ **IP** أو لا سنقوم بدخول على الجهاز الأولى و هو في الشبكة الأولى المسمى **PC 1**.
- الأن هذه الصورة من داخل جهاز الـ **PC1** الذي يقع في داخل الشبكة **192.168.1.0/24**.

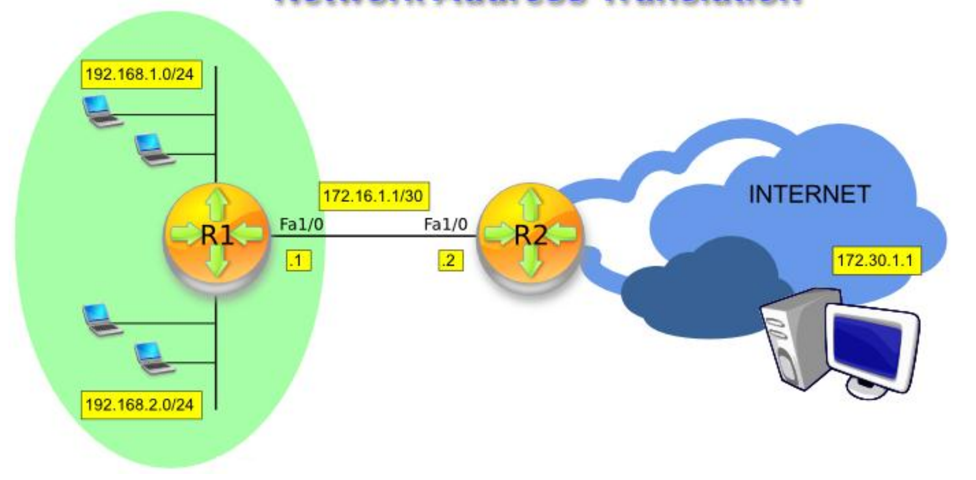


- لاحظ إنه استطاع سحب عنوان **IP** من سيرفر خدمة الـ **DHCP** بهذا الشكل تكون جميع الإعدادات قد تمت بشكل صحيح .
- الأن سنقوم بدخول على جهاز حاسوب المسمى **Laptop 1** موجود في الشبكة الثانية و نتاكد هل تم سحب عنوان **IP** أو لا .



Network Address Translation

(NAT)



NAT : هو عبارة عن بروتوكول يتم تفعيله على جهاز الراوتر الموجود في داخل الشبكة، و وظيفة هذا البروتوكول هي عملية التحويل ما بين العناوين الداخلية الـ **Private IP** و العناوين الخارجية الـ **Public IP**، ويتم تشغيل هذا البروتوكول على مداخل الشبكة المعروفة باسمي البوابة و هي الـ **Defult Gateways** أو على جهاز الفايرول (الجدار الناري) , و هو البروتوكول المستخدم و المعتمد عليه في عملية التحويل ما بين العناوين و الاتصال في الشبكة الخارجية و يوجد ثلاث أنواع من هذا البروتوكول سأقوم بذكرهم و الشرح عنهم لنتعرف عليهم بشكل ممتاز و نستطيع التميز ما بينهم و العمل عليه و سنقوم بتطبيق شبكة عملية لنتعرف ايضاً على إعدادات هذا البروتوكول و كيف تتم عملية تفعيله على راوترات سيسكو .

أنواع بروتوكول الـ NAT :

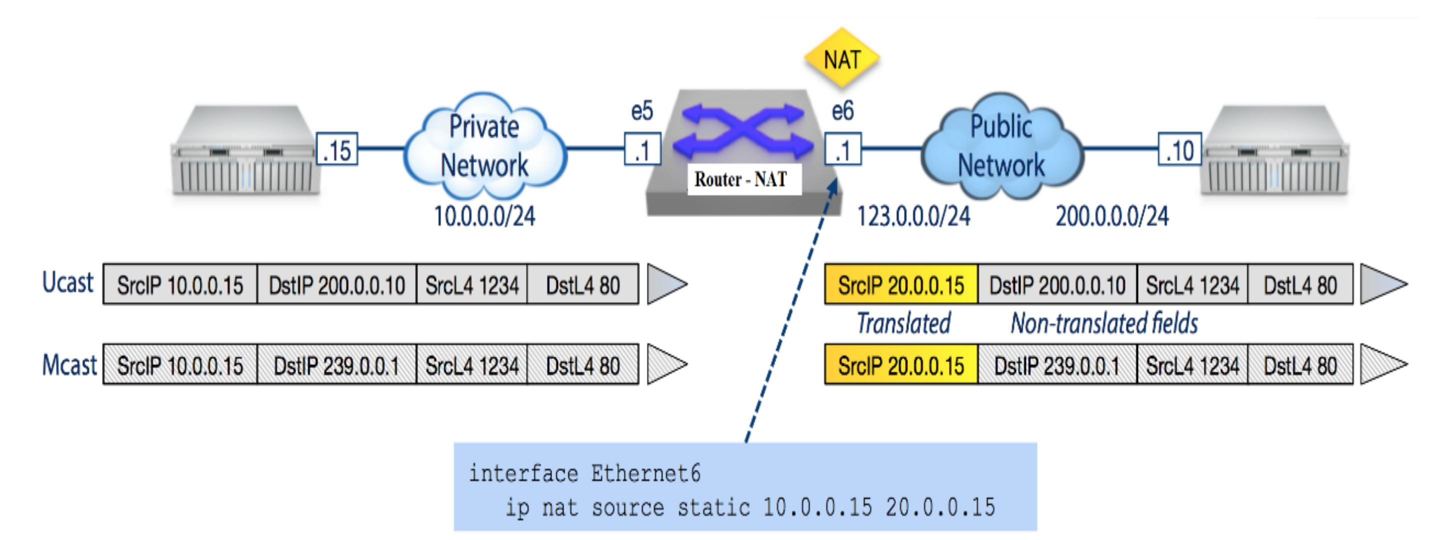
الإعدادات اليدوي	**1- Static – NAT One To One**
الإعدادات الديناميكي	**2- Dynamic – NAT Group To Group**
الإعدادات العام	**3- PAT – NAT One To Group**

- هذه هي الأنواع الثالثة سأقوم بشرح كل نوع بشكل منفرد عن الآخر لنتسطيع فهم الأنواع و نعرف متى نستخدم كل واحد من هذه الأنواع أو متى نريد أو على حسب تصميم الشبكة و نحن سنقوم بتطبيق العملي على هذه الأنواع بشكل عملي .

مميزات و فوائد بروتوكول الـ NAT :

١- أكثر أمان من ناحية الحماية و الاختراق .
٢- تقليل استهلاك عدد العناوين الكثيرة .
٣- اسهل و افضل في عملية تحليل الشبكة و الصيانة .

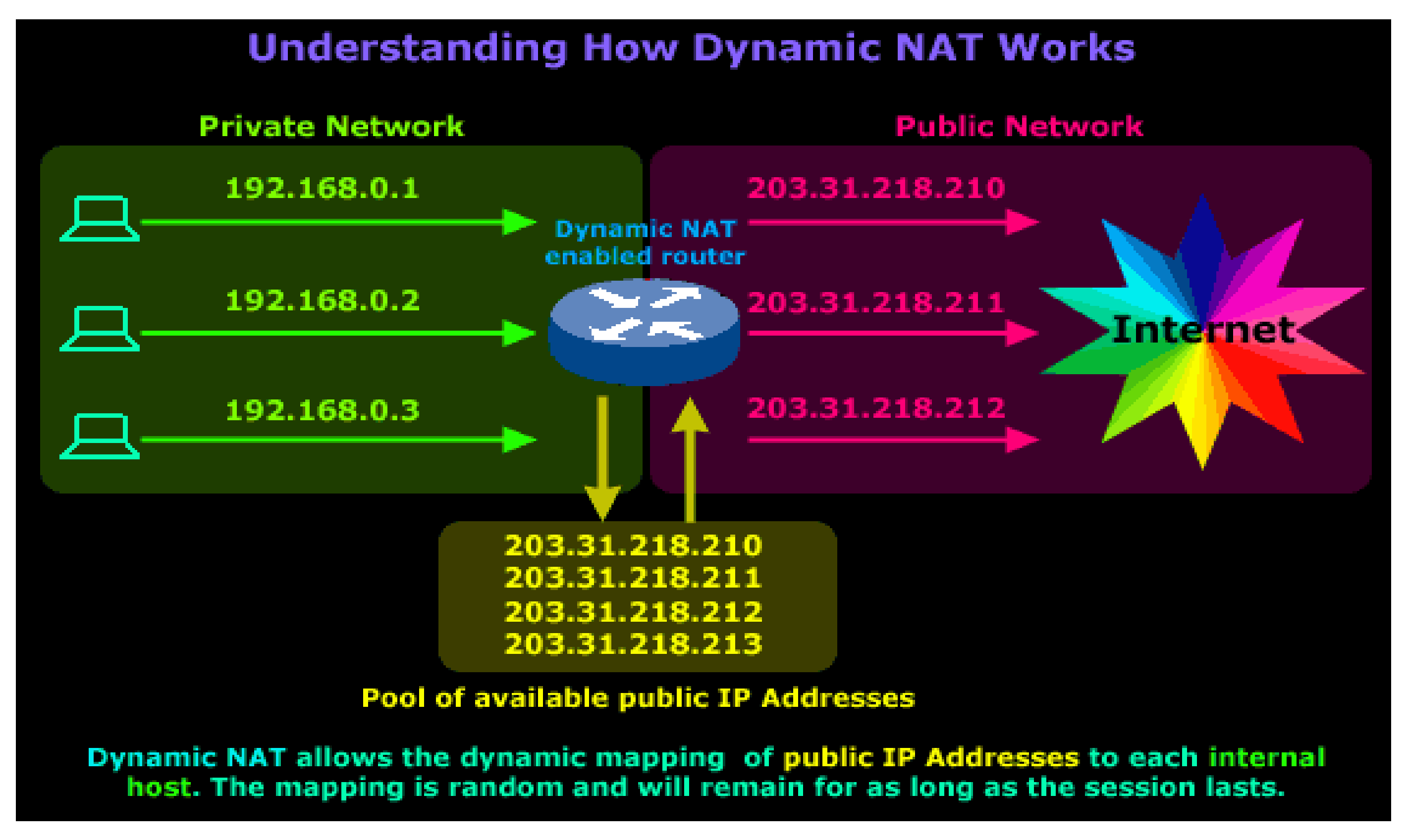
Static – NAT : هذا النوع نقوم بعمله بشكل يدوي مثل عندما ا نريد جهاز حاسوب معين أن يتصل في شبكة الانترنت سنقوم باحضار عنوان الـ **Private IP** نضعه في جهاز الراوتر و سنقوم ايضاً باحضار عنوان الـ **Public IP** و نقوم بدخول على جهاز الراوتر و عمل إعدادات الـ **Static – NAT** ، بمعنى إنه سيكون لكل جهاز في الشبكة عنوان واحد **Private IP** و على الجانب الآخر سيكون ايضاً **Public IP** ليخرج منه على شبكة الانترنت كما في الصورة التالية



- لاحظ في الصورة إنه يوجد لدينا شبكتين شبكة داخلية **Private Network** و شبكة خارجية أو عامة **Public Network** و يوجد في المنتصف جهاز راوتر يقوم بعملية التحويل ما بين العناوين الداخلية و الخارجية , الأن لاحظ إنه في الشبكة الداخلية يوجد جهاز حاسوب ياخذ عنوان **Src 10.0.0.15** طالب الذهاب للعنوان التالي **Dest 200.0.0.10** في هذه الحالة الشبكة الداخلية لا تعرف الشبكة الـ **200.0.0.10** سيتم إرسال العناون الى جهاز الراوتر ليقوم بإرسال ه لشبكة الانترنت هذا الشيء من الطبيعي جداً ولكن عند وصول الرسالة للراوتر سيقوم الراوتر باخذه و تحويله للعنوان الثاني المتصل في الانترنت و هو **123.0.0.0/24** ، و في هذه الحالة هنا ياتي دور بروتوكول الـ **NAT** و هو الذي سيقوم بتحديد عناوين الشبكة الخارجة من الشبكة الداخلية الى الشبكة الخارجية و من اية عنوان تخرج في هذه الحالة سيتم الإرسال و , عند وصول الرسالة و معودة الرد سيتم إرسال الرسالة ايضاً للعناون الـ **10.0.0.15** بهذه الطريقة نحن نعمل بشكل صحيح ولكن يجب أن نعرف إنه تم ضبط العناوين بشكل يدوي بمعنى الجهاز الذي قام بإرسال رسالة لشبكة الانترنت احتاج لعناون شبكة خارجي ليتم تحويله نحن قمنا باحضار عنوان عامة و ضبطها على جهاز الراوتر ، و قمنا ايضاً بتعريف الجهاز صاحب العنوان الداخلي على هذا العناون الخارجي ليخرج منه الى شبكة الانترنت كما هو موضح في الصورة .

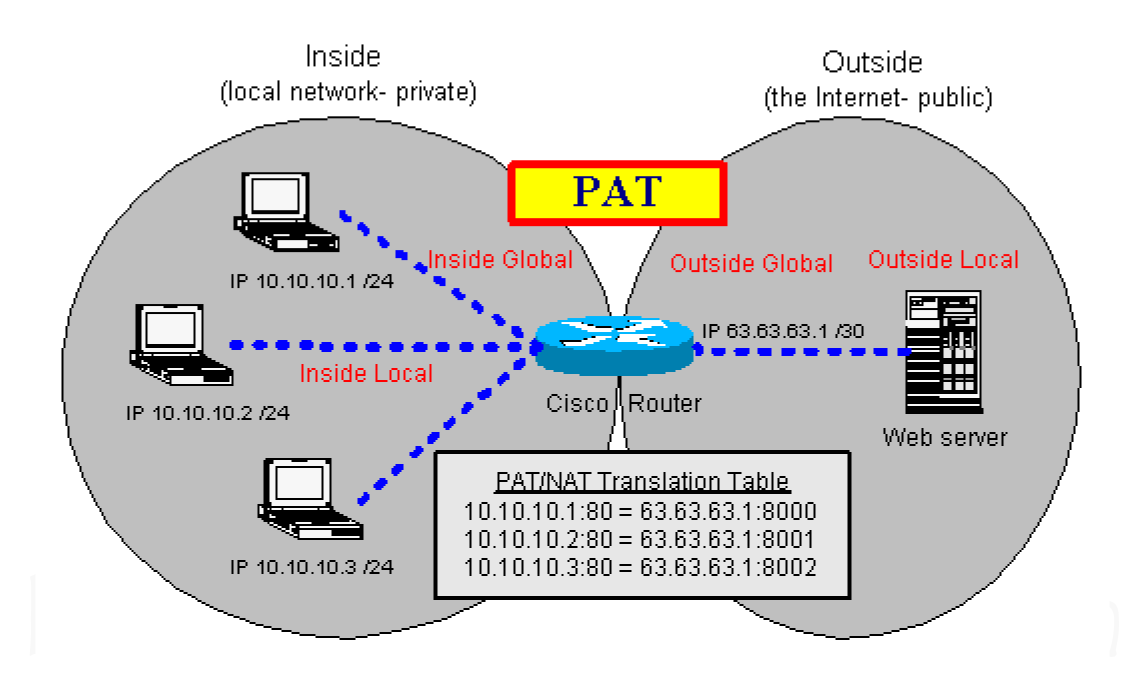
- معلومة بسيطة و بشكل مختصر لنوع الـ **Static – NAT** يعني هذا النوع إنه كل جهاز حاسوب في الشبكة ياخذ عنوان **Private IP** ، و على مقابلة **Public IP** هذا يعني إنه كل جهاز يحتاج عنوان **Public IP** خاص فيه و هذه العملية مكلفة جداً جداً .

Dynamic – NAT : هذا النوع من الـ **NAT** يقوم بعمل مخزن أو **Pool** يتم وضع العناوين العامة الـ **Public IP** التي تم استئجاره من شركة مزودي الخدمة , حيث يتم استخدامهم من قبل أجهزة الحاسوب التي في داخل الشبكة الداخلية عندما يريدون الخروج الى شبكة الانترنت و فكرة هذا النوع إنه يحتوي على اكثر من عنوان عامة و يستطيعون المستخدمين استخدامهم كلهم ، ولكن في حال تم استهلك جميع العناوين و اروده مستخدم الخروج لان يستطيع الخروج لي لأنها لا يوجد عناوين عامة لياخذ عنوان و يخرج فيه على شبكة الانترنت و عليه أن ينتظر لوقت ما ينتهي أحد من استخدام العناون و تركه ليستطيع استخدامه و الخروج على شبكة الانترنت كما في الصورة التالية .



- لاحظ كما هو موضح في الصورة جهاز الراوتر يحتوي على مخزن أو **Pool** و يتحوي في داخله على عنوان عامة **Public IP** , و لاحظ ايضاً إنه يوجد شبكتان شبكة داخلية و شبكة خارجية و عندما يريد جهاز حاسوب من الشبكة الداخلية الخروج لشبكة الانترنت سيقوم بذهاب لبروتوكول الـ **NAT** و سيتم تمريره على الـ **Pool** ياخذ عنوان عامة و يخرج فيه على شبكة الانترنت كما هو موضح في الصورة .
- مثال على ذالك أنظر للصورة ما بين الشبكة الداخلية و الشبكة الخارجية لاحظ إنه الأجهزة التي في الشبكة الداخلية تريد الخروج الى شبكة الانترنت لاحظ إنه يوجد لدينا ثلاث أجهزة حاسوب و يريدون الخروج سيطلبون الخروج على الانترنت من جهاز الراوتر في هذه الحالة جهاز الراوتر سيقوم بإرسال الطلب الى بروتوكول الـ **NAT** و تحويلهم الى المخزم الـ **Pool** ونلاحظ إنه تم اخذ ثلاث عناوين و باقي عنوان واحد في هذه الحالة يستطيع جهاز رابع اخذ هذا العنوان و الخروج على شبكة الانترنت .

PAT – NAT: هذا النوع هو المستخدم بشكل عام في الحياة العملية و هو المعتمد عليه في الشبكات مثل شبكة المنزل أو شبكة المؤسسات أو الشركات، فهو يوفر عدد كبير جداً من العناوين العامة **Public IP**، و فكرة هذا النوع إنه نقوم بتعين عنوان عامة واحد و نجعل جميع الأجهزة التي في الشبكة الداخلية أن تقوم بالاتصال في شبكة الانترنت من خلال هذا العنوان الواحد بغض النظر عن عدد الأجهزة الموجودة في داخل الشبكة، كما في الصورة التالية توضح هذا النوع.

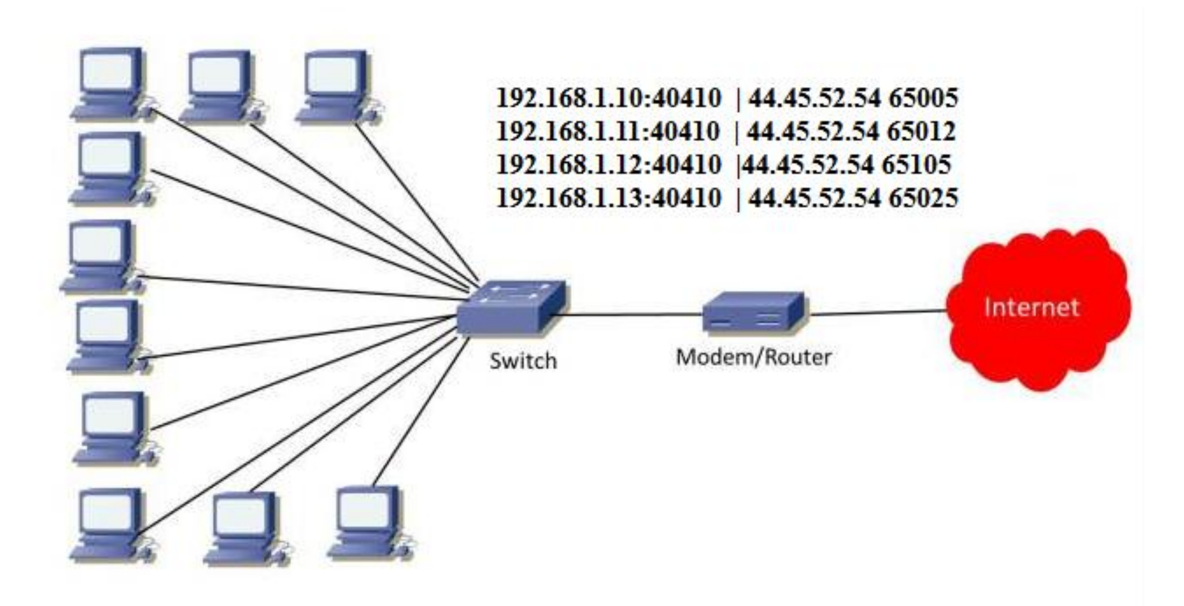


- لاحظ في الصورة إنه يوجد شبكتان شبكة خارجية و شبكة داخلية و يربط ما بينهم جهاز الراوتر و مفعل عليه بروتوكول الـ **NAT – PAT** ، ولكن في هذه الصورة يوجد اكثر من عنوان عامة تم اضافتهم في داخل جدول الـ **NAT** ، ولكن بغض النظر عن عدد العناوين فكرة الـ **NAT – PAT** هو إنه يستطيع أن يجمع عدد كبير من المستخدمين في داخل الشبكة و يجعلهم يتصلون في شبكة الانترنت من خلال عنوان عامة واحد .

- مثال على الشبكة المنزلية : الشبكة المنزلية تعمل ببروتوكول الـ **NAT** و يتم تفعيل بروتوكول الـ **NAT** على المودم الموجود لدينا في المنزل سأقوم بتوضيح العملية التي تعمل فيه هذه الشبكة بشكل مبسط .

- يجب أن نعلم أن المودم الذي نره في المنزل هو ليسه جهاز راوتر بل هو عبارة عن مودم يقوم بتحويل الإشارة و يقوم بوظيفة توصيل الانترنت لديك مع العلم إنه يعمل ببروتوكول مثل الـ **RIP** الاتصال في الراوتر الموجودة في مزود الخدمة الذي انت مشترك معه ، ويجب أن نعلم إنه ايضاً يتم تفعيل بروتوكول الـ **NAT – PAT** حيث يقوم بعمل جدول في داخل المودم يقوم بتسجيل جميع عناوين الأجهزة التي في الشبكة مثل في المنزل يوجد اكثر من جهاز حاسوب يقوم بتسجيل العناوين في هذا الجدول

الموجود في المودم الأن شركة مزود الخدمة تقوم بتزويدينا عنوان عامة واحد فقط يتم تركيبه على المودم و من خلاله تستطيع جميع أجهزة المنزل الخروج على شبكة الانترنت بشكل طبيعي كما في الصورة التالية يظهر فيه جدول يوضح الطريقة .

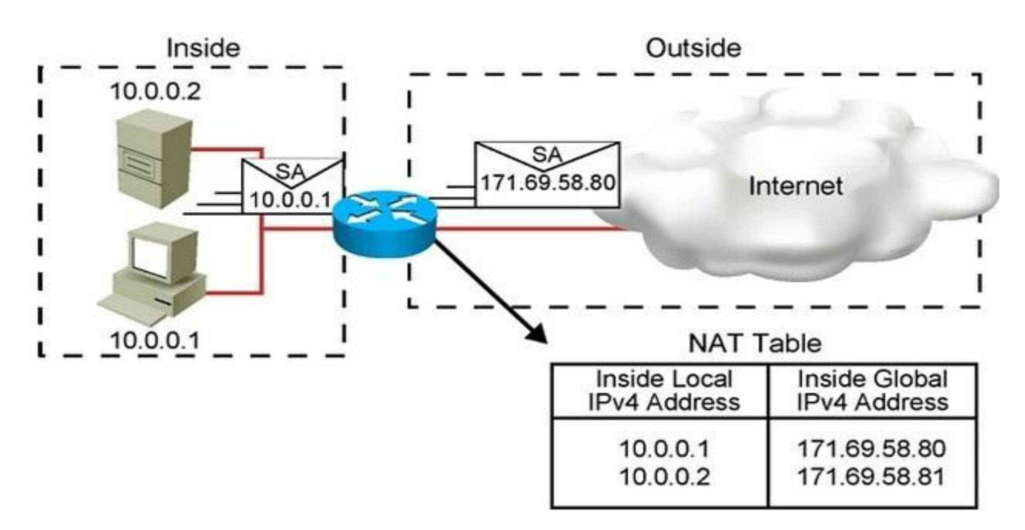


- كما نلاحظ إنه يوجد عدة أجهزة حاسوب و يوجد مودم متصل بشبكة الانترنت الأن في داخل المودم يوجد جدول يقوم بتسجيل جميع عناوين الأجهزة التي متصل في شبكة الانترنت و مقبل كل عنوان خاص في جهاز حاسوب يوجد العناوين العام و هو الذي سيوصل الأجهزة في شبكة الانترنت في هذه الحالة اي جهاز آخر في يريد الخروج على شبكة الانترنت سيتم خروجه عن طريق العناوين العام .

NAT Names

اسماء العناوين في بروتوكول الـ NAT

1- **Global Address = Public Address** **العناوين العامة**
2- **Local Address = Private Address** **العناوين الخاصة**



- كما نلاحظ في الصورة من جهة الشبكة الداخلية تسمى الـ **Inside** و من جهة الشبكة الخارجية تسمى **Outside** ، بمعني إنه الرسالة التي سيتم إرسال ه من الشبكة الداخلية تمسى بهذا الاسم و العكس و هذه العناوين يجب أن نقوم بتحديده في عملية الإعدادات .

إعدادات بروتوكول الـ NAT



Static NAT Configuration

Router > **enable**

Router # **config t**

Router (config) # **ip nat inside source static 192.168.1.9 52.53.54.55**

عنوان الـ **IP** الذي بلون الازرق هو عنوان الـ **IP** العام **Public IP**.

Dynamic NAT Configuration

Router > **enable**

Router # **config t**

Router (config) # **access-list 1 permit 192.168.1.0 0.0.0.255**

Router (config) # **ip nat pool IT 52.53.54.1 52.53.54.40 netmask 255.255.255.0**

هنا نقوم بانشاء المخزن الـ **Pool** و نقوم بتخزين العناوين العامة التي قد تم اخذها من شركة مزود الخدمة **ISP** و مع العلم الـ **netmask** ناخذه مع العنوان و نقوم بوضعه في المخزن الـ **Pool** .

Router (config) # **ip nat inside source list 1 pool IT**

PAT NAT Configuration

Router > **enable**

Router # **config t**

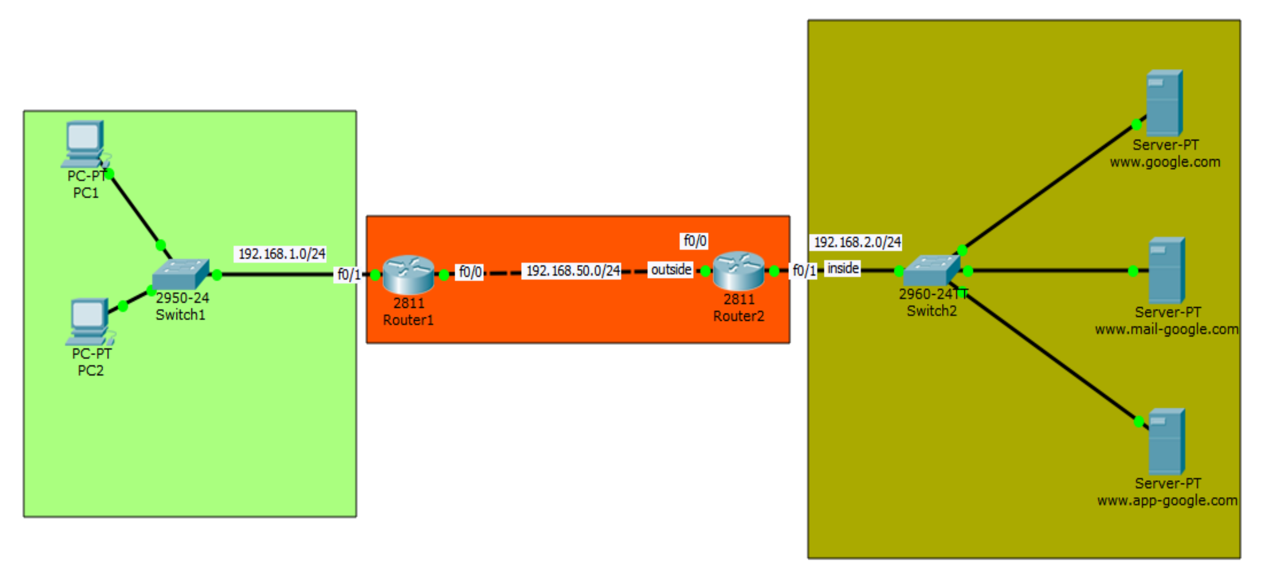
Router (config) # **access-list 1 permit 192.168.1.0 0.0.0.255**

Router (config) # **ip nat pool IT 65.65.65.1 65.65.65.10 netmask 255.255.255.0**

Router (config) # **ip nat inside source list 1 pool IT overload**

- الأن سنقوم ببناء شبكة صغيرة مكون من ثلاث شبكات و سنقوم بتطبيق بروتوكول الـ **NAT – PAT** على الشبكة ولكن قبل أن نبداء يجب أن نتعرف على إعدادات الشبكة.
- الشبكة الأولى بعنوان **192.168.1.0/24** هذه الشبكة الداخلية التي ستتصل في السيرفر الموجود في الشبكة الثالثة .
- الشبكة الثانية بعنوان **192.168.50.0/24** هذه الشبكة التي سترتبط ما بين الشبكات مع بعضهم البعض و سنقوم بتفعيل بروتوكول الـ **RIPv2** ما بين الراوترات .
- الشبكة الثالثة بعنوان **192.168.2.0/24** هذه الشبكة التي تحتوي على السيرفر و التي سنتصل فيه من خلال بروتوكول الـ **NAT** .
- قبل أن نبداء في العمل يجب أن نعرف بعض الملاحظات المهم جداً جداً جداً و يجب أن نكون على معرفة بشكل ممتاز في هذه المعلومات لتجنب المشاكل في العمل قبل البداء في اية مشروع أو اية بناء شبكة يجب أن نقوم بدرسة الكاملة و المعرفة متى سنحتاج هذه الإعدادات و في اية مرحلة سنقوم بها لنعمل بشكل صحيح مثال على ذلك نحن الأن نريد تفعيل بروتوكول الـ **NAT** سنقوم بتفعيله ولكن ماذا نحتاج قبل أن نقوم بتفعيل هذا البروتوكول ، من الطبيعي جداً أن يتواجد اتصال ما بين الراوترات لنستيطع الاتصال في الشبكات الآخر و في هذه الحالة يجب أن نقوم بتفعيل بروتوكول توجيه لجعل

الراوترات تتصل فيه بعضها البعض و بعد هذا ياتي وقت بروتوكول الـ **NAT** لنستطيع



العمل عليه بشكل منظم و صحيح .

ملاحظة مهم جداً جداً : بروتوكول الـ **NAT** لا يقوم بعملية الاتصال و الربط ما بين الراوترات و الشبكات بمعنى إنه يجب أن يتواجد اتصال ما بين الراوترات ليعمل بروتوكول الـ **NAT** بشكل صحيح ، و يجب أن لا نخلط ما بين بروتوكول الـ **NAT** و بروتوكول التوجيه مثل الـ **RIP** .

معلومة مفيدة : مثال على الحياة العملية من الطبيعي إنه يتوجد جهاز مودم لديك لتسطيع الاتصال في الانترنت ، هذا المودم يوجد عليه بروتوكول توجيه و بروتوكول الـ **NAT** لنسطيع الاتصال بشبكة مزودي الخدمة و نستطيع التحويل ما بين العناوين عن طريق الـ **NAT** .

هذا النموذج التالي الذي سنقوم بتطبيق عليه

- الأن سنقوم بدخول على الراوتر الأول **R2** و نقوم بعمل الإعدادات التالية :

- سنقوم بتفعيل منافذ الراوتر و تركيب العناوين على المنافذ و تفعيل بروتوكول الـ **RIPv2** .
- ملاحظة : يجب تحديد نوع المنفذ الذي سيعمل بشكل **outside** , **inside** ليتم التميز ما بينهم و العمل بشكل صحيح .

سنقوم بكتابة الاوامر التالية :

Router > **enable**

Router # **config t**

Router (config) # **interface fastethernet 0/0**

Router (config-if) # **ip address 192.168.50.1 255.255.255.0**

Router (config-if) # **no shutdown**

Router (config-if) # **exit**

Router (config) # **interface fastethernet 0/1**

Router (config-if) # **ip address 192.168.1.1 255.255.255.0**

Router (config-if) # **no shutdown**

Router (config-if) # **exit**

Router (config) # **router rip**

Router (config-router) # **version 2**

Router (config-router) # **network 192.168.50.0**

Router (config-router) # **network 192.168.1.0**

Router (config) # **ip route 0.0.0.0 0.0.0.0 192.168.50.2**

Router (config) # **interface fastethernet 0/1**

Router (config-if) # **ip nat inside**

Router (config-if) # **exit**

Router (config) # **interface fastethernet 0/0**

Router (config-if) # **ip nat outside**

Router (config) # **access-list 1 permit 192.168.2.0 0.0.0.255**

Router (config) # **ip nat pool IT 65.65.65.1 65.65.65.10 netmask 255.255.255.0**

Router (config) # **ip nat inside source list 1 pool IT overload**

Router (config) # **end**

Router # **copy running-config startup-config**

- بهذه الإعدادات تم تفعيل بروتوكول الـ **RIPv2** و **NAT-PAT** و الأن سنقوم بعمل اختبار لنرى هل الشبكات متصلة مع بعضها البعض و هل بروتوكول الـ **NAT-PAT** يعمل بشكل صحيح أو لا ، سنقوم بعمل اختبار لبروتوكول الـ **RIPv2** و نرى هل

الراوترات متصله مع بعضها البعض أو لا و بعده سنقوم بعمل اختبار بروتوكول الـ **NAT-PAT** .

- سنقوم بدخول على راوتر **R1** و سنقوم بكتابة الأمر **Ping** للاتصال في الراوتر **R2**.

```
Router>enable
Router#ping 192.168.50.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.50.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/1 ms

Router#
```

- كما نلاحظ إنه تم الرد من الراوتر **R2** هذا يدل على إنه الإعدادات صحيحة الأن نريد التاكد من جداول التوجيه في الرواترات .
- الأن سنقوم بدخول على الراوتر **R1** و نقوم بعمل عرض لجدول التوجيه .

سنقوم بكتابة الأمر التالي ← Router # **show ip route**

```
Router#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 192.168.50.2 to network 0.0.0.0

C    192.168.1.0/24 is directly connected, FastEthernet0/1
R    192.168.2.0/24 [120/1] via 192.168.50.2, 00:00:05, FastEthernet0/0
C    192.168.50.0/24 is directly connected, FastEthernet0/0
S*   0.0.0.0/0 [1/0] via 192.168.50.2
Router#
```

- لاحظ في جدول التوجيه يوجد رمز **R** هذا اختصار لـ بروتوكول الـ **RIPv2** ، و يوجد ايضاً اختصار الـ **S*** هذا الرمز اختصار لـ إعدادات الـ **default gateway** ، و هذا التوجيه وظيفته عندا طلب عنوان معين مثل فيس بوك أو جوجل أو يوتيوب أو اية عنوان موقع غير موجود في داخل الشبكة الخاصة بينا أو شركة مزود الخدمة سيخرج العنوان على العنوان هذا **0.0.0.0** ، في هذه الحالة يعرف الراوتر إنه يريد الخروج الى شبكة غير معروفة مثل ما ذكرنا على المواقع السابقة .

- الأن سنقوم بدخول على الراوتر **R2** و نقوم بعرض جدول التوجيه لنتاكد من الشبكة هل تم اضافتها أو لا .

Router1

Physical | Config | CLI

IOS Command Line Interface

```
Router#debug ip nat
IP NAT debugging is on
Router#
NAT*: s=192.168.1.1->65.65.60.1, d=224.0.0.9 [1982]

NAT*: s=192.168.1.1->65.65.60.1, d=224.0.0.9 [1984]

NAT*: s=192.168.1.1->65.65.60.1, d=224.0.0.9 [1986]

NAT*: s=192.168.1.1->65.65.60.1, d=224.0.0.9 [1988]

NAT*: s=192.168.1.1->65.65.60.1, d=224.0.0.9 [1990]

NAT*: s=192.168.1.1->65.65.60.1, d=224.0.0.9 [1992]

NAT*: s=192.168.1.1->65.65.60.1, d=224.0.0.9 [1994]

NAT*: s=192.168.1.1->65.65.60.1, d=224.0.0.9 [1996]

NAT*: s=192.168.1.1->65.65.60.1, d=224.0.0.9 [1998]

NAT*: s=192.168.1.1->65.65.60.1, d=224.0.0.9 [2000]

NAT*: s=192.168.1.1->65.65.60.1, d=224.0.0.9 [2002]
```

Copy | Paste

```
Router#
Router#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 192.168.50.1 to network 0.0.0.0

R    192.168.1.0/24 [120/1] via 192.168.50.1, 00:00:24, FastEthernet0/0
C    192.168.2.0/24 is directly connected, FastEthernet0/1
C    192.168.50.0/24 is directly connected, FastEthernet0/0
S*   0.0.0.0/0 [1/0] via 192.168.50.1
Router#
```

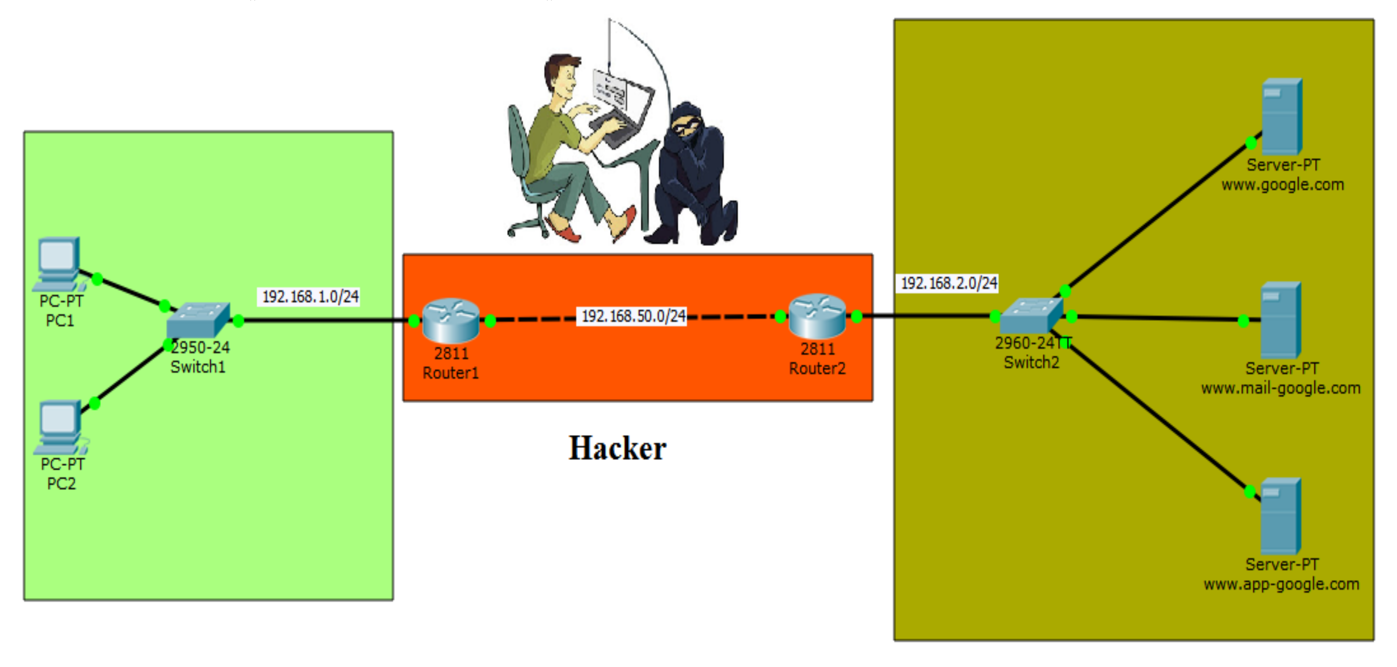
- كما نلاحظ أن الشبكة الموجودة في جدول توجيه الـ **R1** موجودة في جدول توجيه الراوتر **R2** ، بهذا الشكل نكون قد تاكدنا من الاتصال ما بين الراوتر بشكل صحيح الأن علينا أن نقوم باختبار بروتوكول الـ **NAT – PAT** هل يعمل أو لا .
- الأن سنقوم بعمل الاختبار عن طريق إرسال **Packet** من جهاز المستخدم الموجود في شبكة **192.168.1.0/24** الى السيرفر الموجود في شبكة **192.168.2.0/24** ، و سنقوم بتفعيل امر مهم جداً على الراوتر **R1** لنرى كيف ستتم عملية التحويل في بروتوكول الـ **NAT – PAT** ما بين العناوين الداخلي و العناوين الخارجي ، الأن سنقوم بكتابة الأمر التالي . Router # **debug ip nat** هذا الأمر مهم جداً جداً جداً و هو الذي يظهر لك عملية التحويل ما بين العناوين، كما في الصورة التالية من داخل الراوتر.
- لاحظ هذا من داخل الراوتر تم تحويل العناوين ، بمعنى إنه تم تحويل العنوان الداخلي الخاص في الشبكة **192.168.1.1** الى عنوان عام و هو **65.65.60.1** هذا العنوان الذي عن طريقه نستطيع الخروج الى شبكة الانترنت العامة .
- نظرة من جهة أمنية لهذه التقنية :

- تقنية الـ **NAT** بشكل عام هي مختصة ايضاً في حماية الشبكة من الاختراق ، مثل عندما ا نريد إرسال رسالة الى شبكة معينة سيتم إضافة عنوان الجهاز أو السيرفر الداخلي الموجود في الشبكة في الـ **Packet** هذه الحالة نحن في خطر كبير من معرفة عنوان الـ **IP** للخادم أو الجهاز ، ولكن في بروتوكول الـ **NAT** يقوم بتحويل العناوين بمعنى يتم استبداله عند الخروج ، و في حال تم اختراق الخط أو عمل تحليل للخط سيجد العنوان العام بدل من العنوان الداخلي الخاص في الخادم الموجود في داخل الشبكة و بهذه الطريقة نحن قد تمكنه من حماية العنوان و عدم معرفة العناوين الخاصة التي في الشبكة الداخلية ، ولكن هذا لا يعني أن نكون في حماية كاملة في عملية الاختراق اكبر بكثير من هذه الامور .

First Hop Redundancy Protocols = FHRP

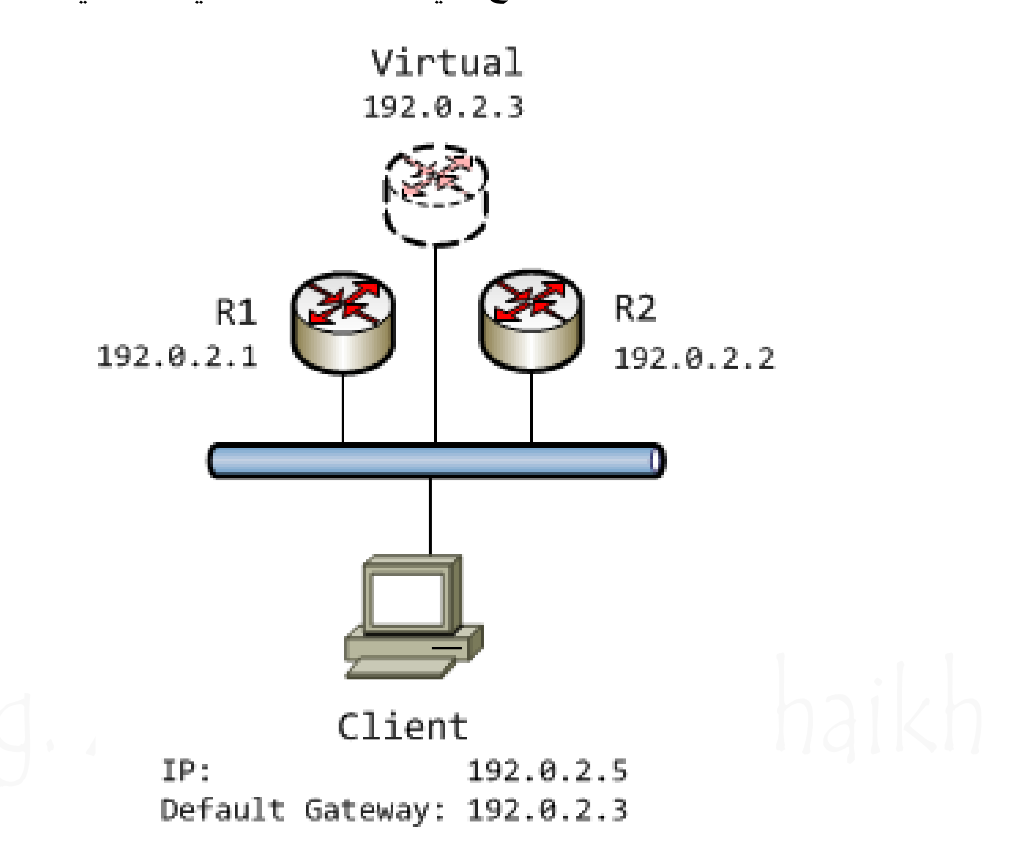
FHRP

FHRP: هذا البروتوكول فكرته انشاء راوتر وهمي أو افتراضي موجود في الشبكة ولكن غير مرائي، ويكون قيد العمل و هو مثل الراوتر الحقيقي الذي يكون موجود في الشبكة و يحتوي على عنوان **IP** مثل باقي الراوتر،و وظيفته عدم توقف الشبكة عن العمل في حال حدث انقطاع أو فصل لي أحد الراوتر الموجودة على الشبكة سيبقى هذا الراوتر الوهمي قيد العمل من دون أن نشعر إنه أحد تعطل أو حصل توقف في أحد أجهزة الراوتر في الشبكة



، و يحتوي هذا البروتوكول على عدة أنواع من البروتوكولات التي يتم تفعيلها على أجهزة الراوترات سأقوم بذكره هذه الأنواع .

- النموذج التالي يوضح فكرة الراوتر الوهمي فهو غير مرئي كما هو واضح في النموذج، ولكن ياخذ عنوان **IP** من نفس الرنج التي تاخذه الراوتر التي تعمل في داخل الشبكة .



- أنواع البروتوكولات التي تعمل تحت نطاق بروتوكول الـ **FHRP** :

FHRP'S
HSRP | VRRP
GLBP

1- **Hot Standby Router Protocol (HSRP)**
2- **Virtual Router Redundancy Protocol (VRRP)**
3- **Gateway Load Balancing Protocol (GLBP)**

- هذه هي أنواع البروتوكولات التي تندرج تحت بروتوكول الـ **FHRP** سأقوم بشرح كل واحد من هذه البروتوكولات بشكل منفرد عن الآخر لنفهم كل واحد كيف يعمل و ما هي مميزاته عن البروتوكول الآخر .

HSRP: هو عبارة عن بروتوكول خاص لشركة سيسكو، ولقد قامة الشركة بتطوير هذا البروتوكول ليكون افضل مما سبق و وظيفة هذا البروتوكول انشاء بوابة وهمية في الشبكة معنى بوابة **Gateway** وهمي يتم إعداداه على أجهزة الراوتر الموجودة في الشبكة في حال توقف راوتر عن العمل أو تم فصل أحد الراوتر عن الآخر أو اية مشكلة تخص الراوترات ، ستبقى الشبكة تعمل بشكل طبيعي جداً حتى ولو كان أحد الراوتر معطل لان تتوقف الشبكة عن العمل لأنه يوجد بوابة وهمية تم تفعيلها على أجهزة الراوتر بعنوان **IP** واحد تعرفه جميع الشبكات الموجودة في الشبكة ، و تحت هذا العنوان جميع الراوتر التي في الشبكة مما ايضاً يفيد هذا الموضوع في توزيع الترافيك في الشبكة ما بين المسارات بدل من أن يكون مسار واحد و عليه ضغط كبير من الترافيك سأقوم بشرح إعدادات هذا البروتوكول على نموذج بشكل عملي لنفهم طبيعة العمل كيف تتم بشكل ممتاز .

- **HSRP** : بشكل مختصر هو يقوم بفكر الراوتر الاحتياطي و الراوتر الرائيسي في حال تم تعطل أحد الراوتر سيبداء الراوتر الثاني بالعمل بدل من تعطل الشبكة.

- **HSRP version**: اصدارات بروتوكول الـ **HSRP** يوجد اصدران و كل اصدار يدعم مميزات و إضافة تختلف بعض اشيء.

- **HSRP version 1**

يعمل مع عناوين الإصدار الرابع **IPv4** و يحتوي على مجموعة عناوين **224.0.0.2 all routers** يدعم جميع مسارات الراوترات و يعمل مع بروتوكول الـ **UDP Port 1985** و يحتوي على عنوان ماك ادرس وهمي **(00:00:0c:07:ac:XX)** ، هذه التقنية موجودة في الإصدار الأول ولكن بعد أن تم تطويره للاصدار الثاني تم إضافة و تحسين هذه التقنية بشكل افضل .

- **HSRP version 2**

هذا الإصدار الثاني بعد التطوير و التحسين عليه اصبح يعمل مع عناوين الإصدار الرابع **IPv4** و الإصدار السادس **IPv6** و ايضاً يحتوي على مجموعة عناوين فقط مختصة في بروتوكول الـ **IPv4 224.0.0.102 (HSRP)** ، **IPv6 ff02::66** و يعمل ايضاً مع بروتوكول **UDP Port 1985** ، و يحتوي على عنوانين ماك ادرس واحد للاصدار الرابع **IPv4 00:00:0c:9f:fX:XX)**، و واحد للاصدار السادس **(00:05:73:a0:0X:XX)** **IPv6**.

- **تسمية الراوترات في بروتوكول الـ HSRP :**

Actice : هو الذي سيكون الراوتر الرائيسي في الشبكة و هو الراوتر الأول في الشبكة

Standby : هو الذي سيكون الراوتر الاحتياطي في الشبكة الذي في حال تم تعطيل الراوتر الرائيسي هذا الراوتر هو الذي سيقوم بدور الراوتر الرائيسي.

- كيف تتم عملية انتخاب الراوتر الرائيسي الذي سيكون **Actice** ستتم هذه العملية عن طريق اقل قيمة **priority** في الراوتر ليتم تعينه الراوتر الرائيسي **Actice** .

- **توقيت رسالة الترحيب في بروتوكول الـ HSRP :**

- عندما ا نقوم بتفعيل بروتوكول الـ **HSRP** على الراوترات ، ستبداء الراوترات بإرسال رسالة ترحيب لجميع الراوترات المتصلة في الشبكة كل **10** ثواني ، على العنوان **224.0.0.2 all routers** ليقوم بتاكيد على الراوترات إنها موجودة في الشبكة أو لا .

إعدادات بروتوكول الـ HSRP

HSRP Configuration

Router > **enable**

Router # **config t**

Router (config) # **interface fastethernet 0/1**

Router (config-if) # **standby 1 priority 90**

Router (config-if) # **standby 1 ip 10.0.0.0** ← **Virtual IP**

Router (config-if) # **standby 1 preempt** ← **Group**

- الأن بعد أن تعرفنا على بروتوكول الـ **HSRP** و إعداداته سنقوم بعمل تطبيق عملي على شبكة مكونه من راوترين ، و سنقوم بتفعيل بروتوكول الـ **HSRP** على الراوترات سنتعرف على الإعدادات .

- **إعدادات الشبكة التي سنعمل عليه التطبيق :**
- الشبكة الأولى تاخذ عنوان **192.168.1.0/24** هذه الشبكة الأولى.
- الشبكة الثانية تاخذ عنوان **192.168.2.0/24** هذه الشبكة الثانية .

- **تقسيم منافذ الراوترات على حسب عناوين الشبكات :**

١- الراوتر الأول **R1** المنفذ **f 0/0** ياخذ عنوان **192.168.1.3/24** و المنفذ **f 0/1** ياخذ عنوان **192.168.2.2/24** .

٢- الراوتر الثاني **R2** المنفذ **f 0/0** ياخذ عنوان **192.168.1.2/24** و المنفذ **f 0/1** ياخذ عنوان **192.168.2.3/24** .

٣- العناوين الافتراضي **Virtual IP** في الشبكة الأولى سيكون **192.168.1.1/24** و في الشبكة الثانية **192.168.2.1/24**.

- **ملاحظة مهم جداً جداً:** أجهزة المستخدمين ستكون عنوان البوابة الـ **Gy** للشبكة الأولى هو **192.168.1.1** و الشبكة الثانية ستكون عنوان البوابة الـ **Gy** للشبكة الثانية **192.168.2.1**.

النموذج التالي هو الذي سنقوم بتطبيق عليه و العمل عليه

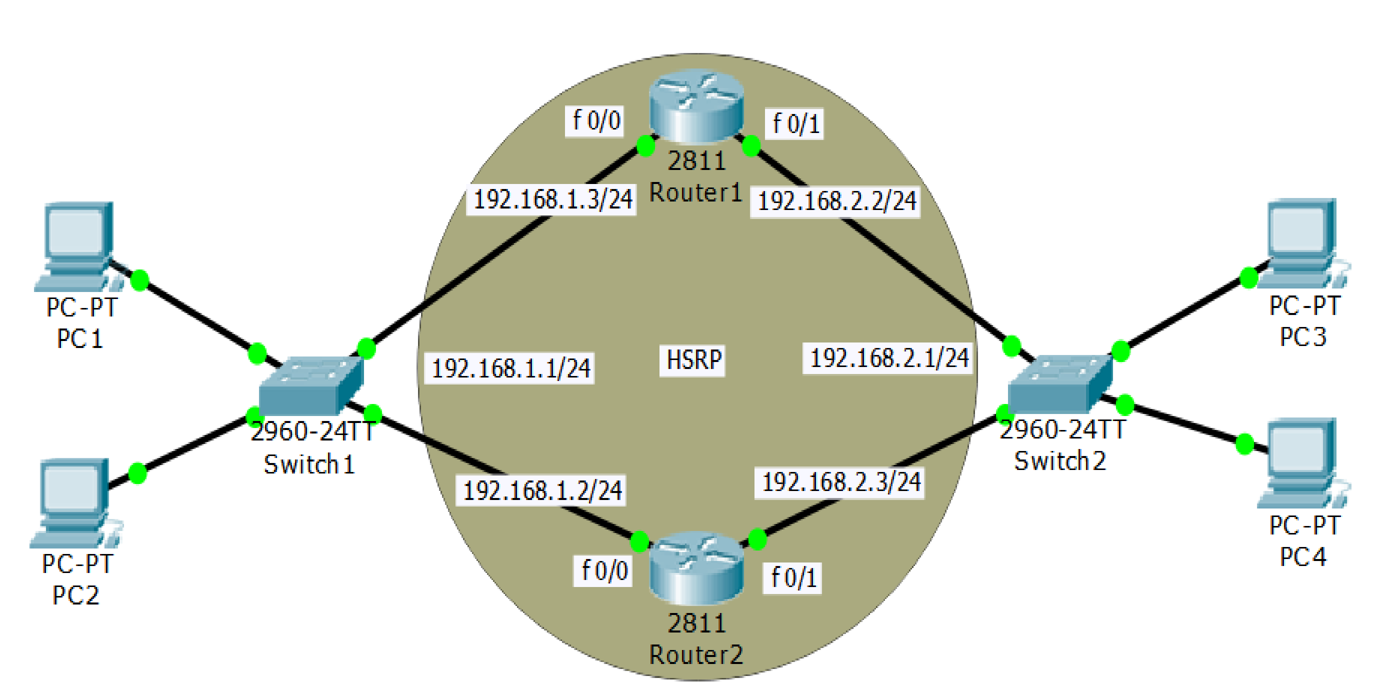
- الأن بعد أن تعرفنا على إعدادات الشبكة سنقوم بدخول على الراوتر **R1** الأول و نقوم بعمل الإعدادات و تفعيل بروتوكول الـ **HSRP** و تفعيل منافذ الراوترات .

سنقوم بكتابة الإعدادات التالية :

Router > **enable**

Router # **config t**

Router (config) # **interface fastEthernet 0/0**



Router (config-if) # **ip address 192.168.1.3 255.255.255.0**

Router (config-if) # **no shutdown**

Router (config-if) # **exit**

Router (config) # **interface fastEthernet 0/1**

Router (config-if) # **ip address 192.168.2.2 255.255.255.0**

Router (config-if) # **no shutdown**

Router (config-if) # **exit**

Router (config) # **interface fastEthernet 0/0**

Router (config-if) # **standby 1 ip 192.168.1.1** ← **Virtual IP**

Router (config-if) # **standby priority 90**

Router (config-if) # **standby 1 preempt** ← **Group**

Router (config-if) # **exit**

Router (config) # **interface fastEthernet 0/1**

Router (config-if) # **standby 1 ip 192.168.2.1** ← **Virtual IP**

Router (config-if) # **standby priority 90**

Router (config-if) # **standby 1 preempt** ← **Group**

Router (config-if) # **end**

Router # **copy running-config startup-config**

- هذه إعدادات الراوتر الأول **R1** الأن سنقوم بدخول على الراوتر الثاني **R2** .
- الأن سنقوم بدخول على الراوتر الثاني **R2** سنقوم بعمل الإعدادات التالية :

سنقوم بكتابة الإعدادات التالية :

Router > **enable**

Router # **config t**

Router (config) # **interface fastEthernet 0/0**

Router (config-if) # **ip address 192.168.1.2 255.255.255.0**

Router (config-if) # **no shutdown**

Router (config-if) # **exit**

Router (config) # **interface fastEthernet 0/1**

Router (config-if) # **ip address 192.168.2.3 255.255.255.0**

Router (config-if) # **no shutdown**

Router (config-if) # **exit**

Router (config) # **interface fastEthernet 0/0**

Router (config-if) # **standby 1 ip 192.168.1.1**

Router (config-if) # **standby priority 90**

Router (config-if) # **standby 1 preempt**

Router (config-if) # **exit**

Router (config) # **interface fastEthernet 0/1**

Router (config-if) # **standby 1 ip 192.168.2.1**

Router (config-if) # **standby priority 90**

Router (config-if) # **standby 1 preempt**

Router (config-if) # **end**

Router # **copy running-config startup-config**

- بهذه الإعدادات نكون قد فعلاً منافذ الراوترات و تم تفعيل بروتوكول الـ **HSRP** على الراوترين **R1** و **R2** وسنقوم بعمل اختبار للشبكة لنتاكد هل كل الإعدادات صحيح أولا ، الأن سأقوم بشرح النموذج بشكل مفصل لنعرف ما فائدة هذا البروتوكول بشكل ممتاز و نريد ايضاً معرفة الراوتر الرائيسي الـ **Actice** .

- الأن في هذه الحالة نحن قمنا بعمل ما يسمى تجاوز توقف الشبكة عن العمل ، لقد قمنا بوضع العناون الوهمي الذي هو البوابة **Gy** على أجهزة الحاسوب الموجودة في الشبكة و من الطبيعي جداً أن أجهزة الحاسوب أن تتصل مع بعضها البعض حتى لو كانت الشبكة مختلفة ولكن ، في هذه الحالة نحن قمنا بوضع عنوان و همي افتراضي للراوترات و هو الذي يربط الراوتر كلها تحت عنوان واحد في حال تم تعطل أحد الراوتر لان تتوقف الشبكة عن العمل بلا ستبقى تعمل بشكل طبيعي و من دون أن يشعر أحد إنه تم تعطل أحد الراوتر في الشبكة .

- الأن سنقوم بكتابة امر يقوم بعرض العناوين الوهمية أو الافتراضية لنرى ما هي طبيعة الشبكة لدينا .

سنقوم بدخول على الراوتر الأول و نقوم بكتابة الأمر التالي :

Router # **show standby brief**

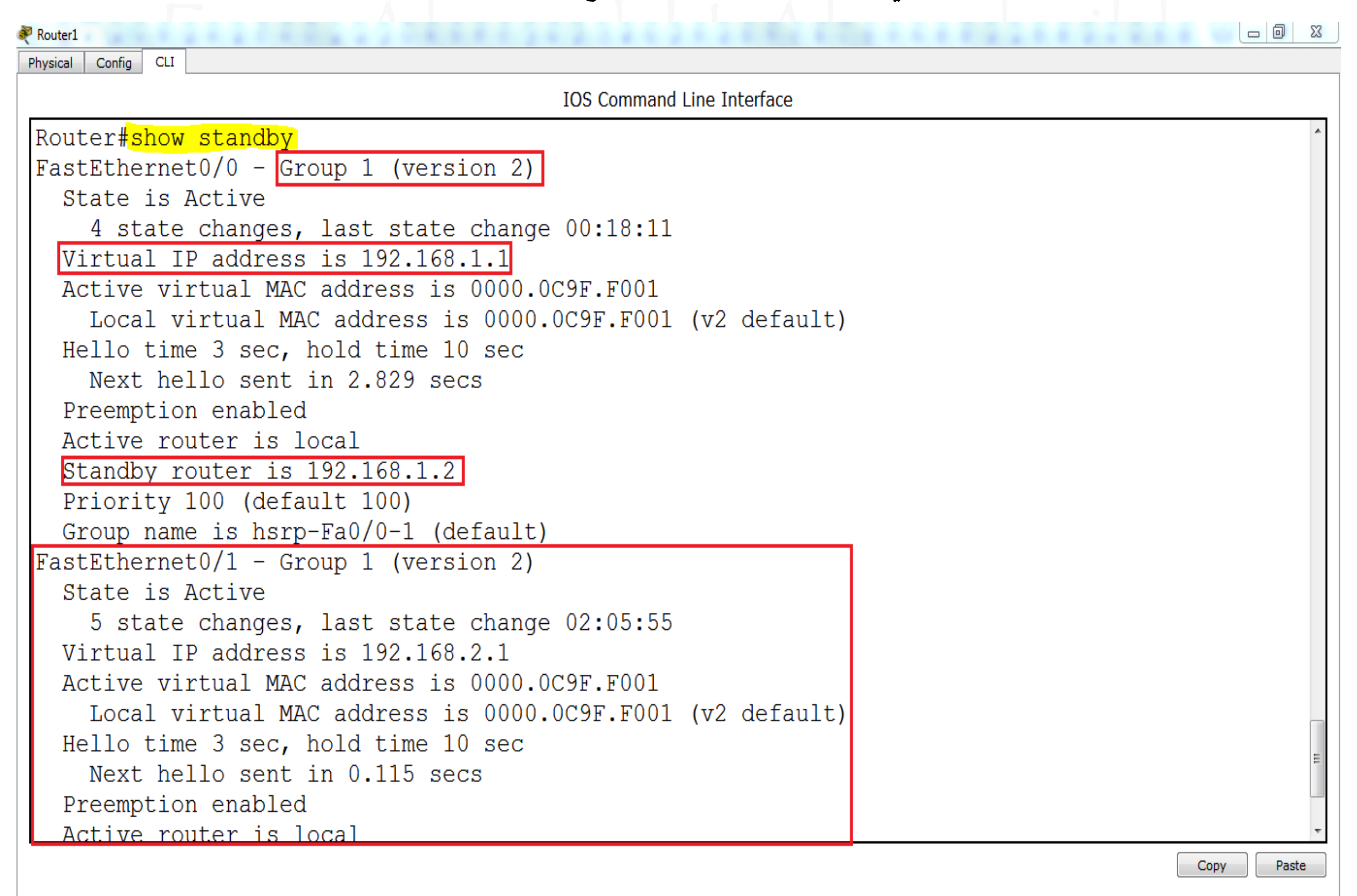
```
Router#show standby brief
                     P indicates configured to preempt.
                     |
Interface   Grp  Pri P State    Active          Standby         Virtual IP
Fa0/0       1    100 P Active   local           192.168.1.2     192.168.1.1
Fa0/1       1    100 P Active   local           192.168.2.3     192.168.2.1
Router#
```

هذه الصورة من داخل الراوتر الأول **R1** لاحظ إنه يوجد **Virtual IP** عناوين وهمية أو افتراضية و هذا ما قمنا به في الإعدادات السابقة ، لو في حال تعطل أحد الراوتر ستبقى تعمل الشبكة بشكل طبيعي لي إنه سيتم تحويل المسار للراوتر الثاني **R2** .

الأن سنقوم بعرض معلومات كاملة عن إعدادات بروتوكول الـ **HSRP** على الراوتر الأول **R1** سنقوم بكتابة الأمر التالي :

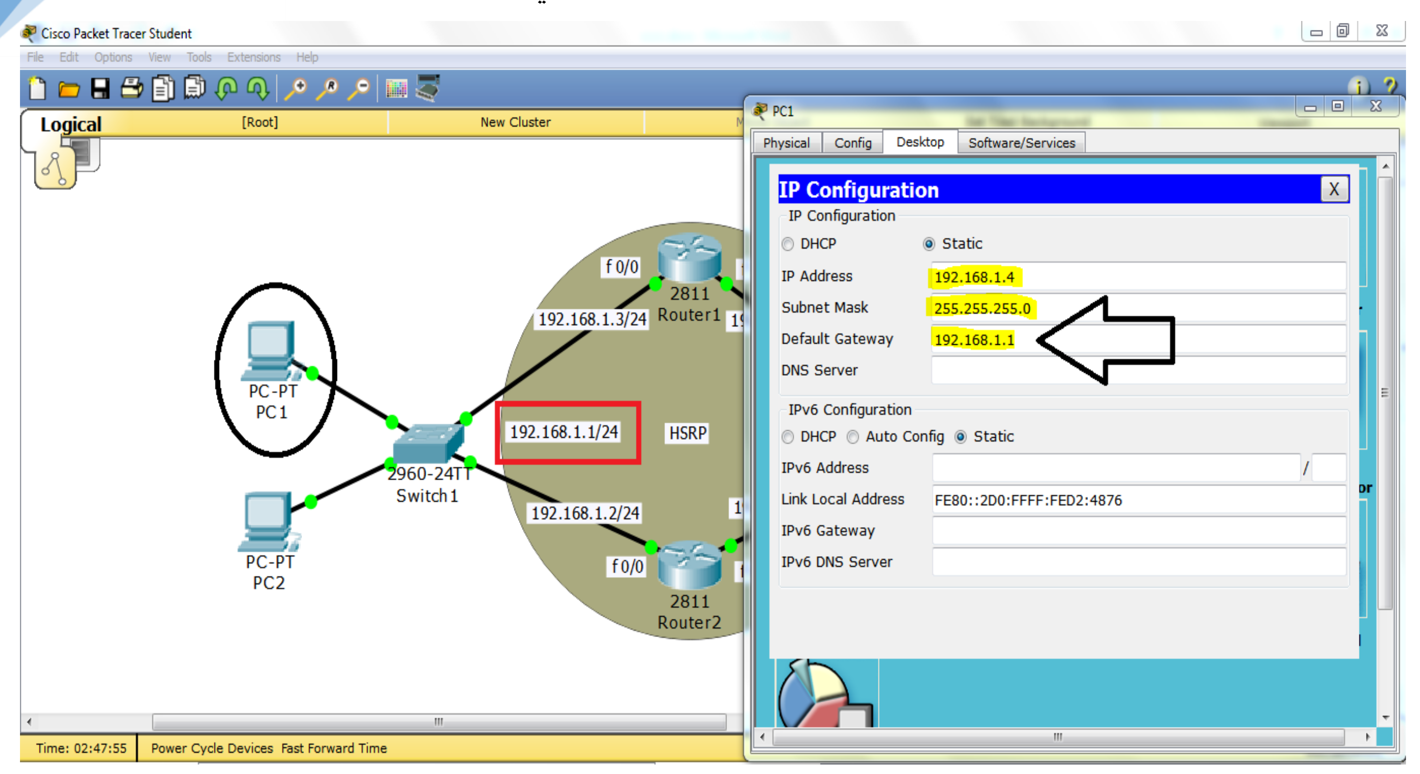
Router # **show standby**

كما نلاحظ في الصورة التالية هذه جميع معلومات البروتوكول




```
Router#show standby
FastEthernet0/0 - Group 1 (version 2)
  State is Active
    4 state changes, last state change 00:18:11
  Virtual IP address is 192.168.1.1
  Active virtual MAC address is 0000.0C9F.F001
    Local virtual MAC address is 0000.0C9F.F001 (v2 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 2.829 secs
  Preemption enabled
  Active router is local
  Standby router is 192.168.1.2
  Priority 100 (default 100)
  Group name is hsrp-Fa0/0-1 (default)
FastEthernet0/1 - Group 1 (version 2)
  State is Active
    5 state changes, last state change 02:05:55
  Virtual IP address is 192.168.2.1
  Active virtual MAC address is 0000.0C9F.F001
    Local virtual MAC address is 0000.0C9F.F001 (v2 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 0.115 secs
  Preemption enabled
  Active router is local
```

- الأن نريد أن ننظر الى اعدادا أحد أجهزة الحاسوب في الشبكة :



كما نلاحظ في الصورة التالية هذه إعدادات أحد أجهزة الحاسوب الموجودة في شبكة الأولى:

- كما نلاحظ في الصورة السابقة إنه تم وضع عنوان البوابة الـ **Gy** العنوان الافتراضي و هو الـ **192.168.1.1** و هذا هو العناون الوهمي الذي يتصل في الراوتر الأول و الراوتر الثانية ، و في حال تم ايقاف أحد الراوتر لا تتوقف الشبكة عن العمل ستبقى تعمل بشكل طبيعي جداً لأنه إنه العنوان الافتراضي يعمل على الراوتر بشكل وهمي .

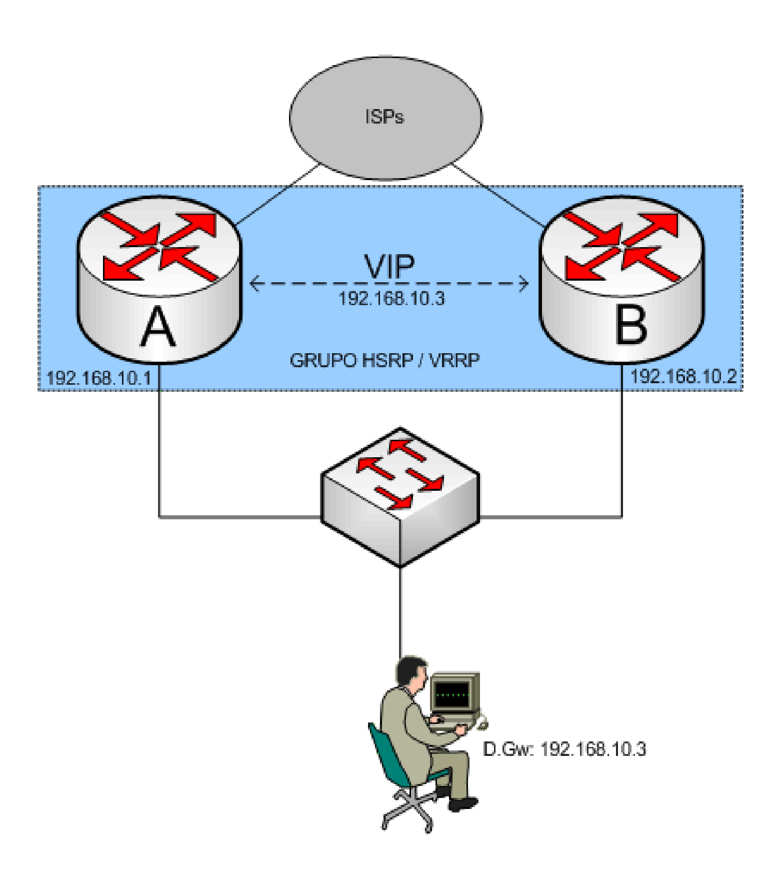
VRRP: هذا البروتوكول هو مفتوح المصدر و فكرته نفس فكرة الـ **HSRP** ولكن يختلف في بعض الميزات البسيطة سأقوم بذكرها، ويجب أن نعرف أن هذا البروتوكول ليسه من شركة سيسكو ولكن يعمل مع جميع أجهزة الراوترات مثل سيسكو و جنيبرا.

ميزات هذا البروتوكول عن بروتوكول الـ **HSRP** اختلف في اسماء أو مصطلحات الراوترات سأقوم بتوضيح الفروق :

الراوترات في بروتوكول الـ **HSRP** تمسى **Active** هذا يعني الراوتر الرائيسية و الراوتر الاحتياطي يسمى **Standby** .

اما في بروتوكول الـ **VRRP** تسمى الراوترات الرائيسي **Master** و الراوتر الاحتياطي يسمى **Backup** .

Active = Master, Standby = Backup



- يعمل مع بروتوكولات الـ **OSPF and EIGRP using IP Protocol**
- يحتوي على ماك ادرس وهمي ايضاً خاص فيه

Virtual Mac Address = 00-00-5E-00-01-XX

- يرسال رسالة الترحيب **Hello Packet** على عنوان **224.0.0.18**

إعدادات بروتوكول الـ VRRP

VRRP Configuration

Router > **enable**

Router # **config t**

Router (config) # **interface fastethernet 0/1**

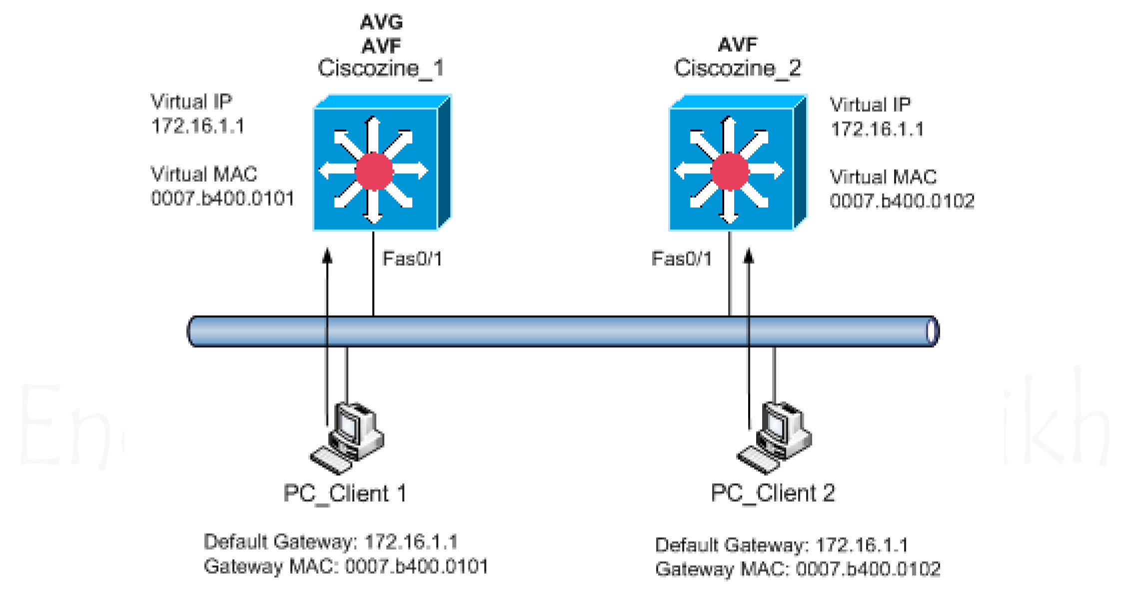
Router (config-if) # **vrrp 1 priority 90**

Router (config-if) # **vrrp dby ip 11.1.1.1**

Router (config-if) # **vrrp 1 preempt**

GLBP: هذا البروتوكول يختلف بشكل كبير جداً عن باقي البروتوكولات التي قمنا بذكرها من قبل فهذا البروتوكول يعمل في الطبقة الثانية من طبقة الـ **OSI**، و يعمل ايضاً على توزيع الترافيك في الشبكة **Load Balancing** و هو مكلية لشركة سيسكو، و اسماء الراوترات تختلف تماماً عن البروتوكولات السابقة سأقوم بذكرهم .

- **Active Virtual Gateway (AVG)** هذا الراوتر الرائيسي.
- **Active Vritual Forword (AVF)** هذا الراوتر الاحتياطي.
- يعمل على إرسال رسالة الترحيب على العنوان **224.0.0.102 Multicast ip** .
- يستخدم بروتوكول الـ **UDP Port 3222** .
- **Mac Address 0007.B400.XXYY**.



إعدادات بروتوكول الـ GLBP

GLBP Configuration

Router > **enable**

Router # **config t**

Router (config) # **interface fastethernet 0/0**

Router (config-if) # **glbp 1 priority 100**

Router (config-if) # **glbp ip 12.1.1.1**

Router (config-if) # **glbp 1 preempt**

Network Time Protocol (NTP)

بروتوكول ضبط الوقت في الشبكة



NTP : هو بروتوكول يقوم بضبط و توزيع الوقت في الشبكة بشكل تلقائي عن طريق مزامنة ساعة الحاسوب, المرتبط في في الشبكة مثل الخادم أو جهاز مختص لضبط الوقت.

- بروتوكول الـ **NTP** يستخدم بروتوكول الـ **UDP** و يعمل على بورت **123**.

إعدادات بروتوكول الـ NTP

NTP Configuration

Router > **enable**

Router # **config t**

Router (config) # **ntp server 192.168.1.100**

Router (config) # **ntp authentication-key 1 md5 cisco**

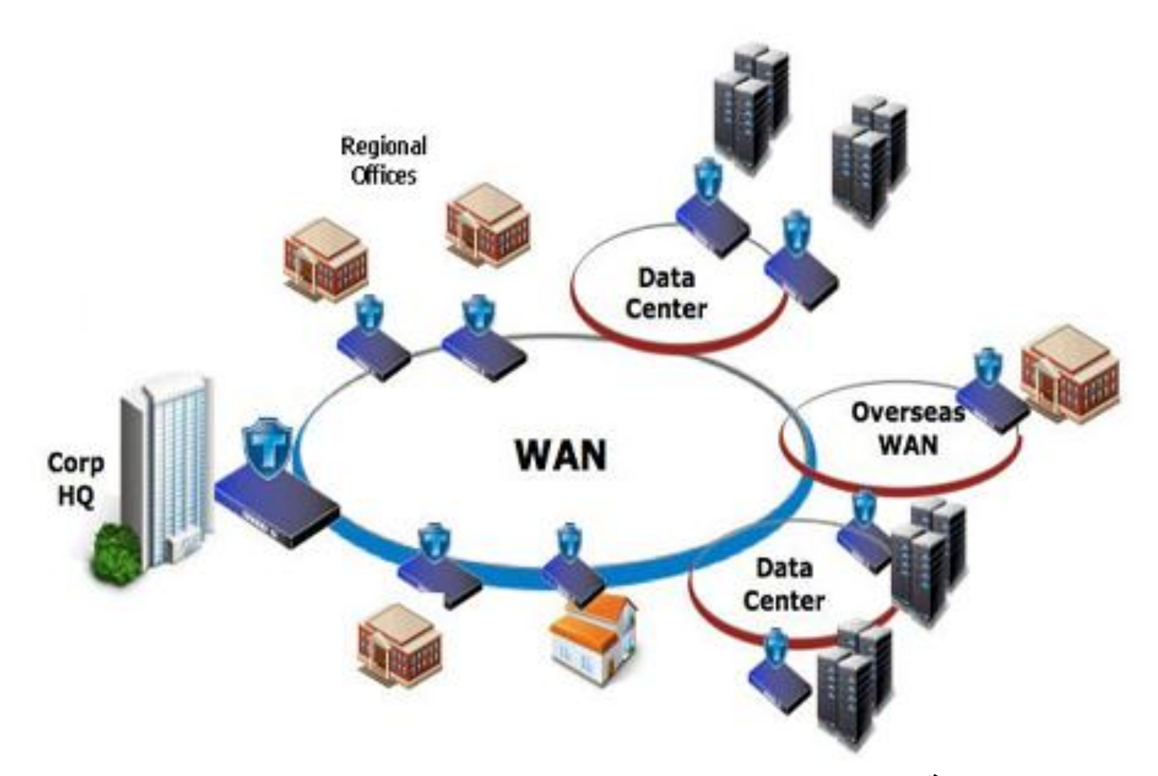
Router (config) # **ntp update-calendar**

- **ملاحظة :** نستطيع ايضاً أن نقوم بضبط الوقت عن طريق السيرفر الموجود في الشبكة أو عن طريق الراوتر أو عن طريق جهاز خاص في ضبط الوقت كما في الصورة التالية :



فهرس المستوى الرابع الشبكة الواسعة WAN

Wide Area Networks (WAN)



الشبكات الواسعة WAN : هذه الشبكة تغطي مساحة جغرافية واسعة وغير محدودة لتوصيل وربط الشبكات المحلية مع بعضها البعض ، مثلاً عندما ا يكون لدينا مؤسسة أو شركة و لديها عدة فروع في دول العالم و نريد الاتصال بهذه الافرع من الطبيعي أن هذه الافرع تنفصل ما بينهم شبكات كثيرة وعدة دول و مسافة كبيرة أيضاً في هذه حالة عندما ا نريد الاتصال بأحد الأفرع البعيدة فإن الاتصال سيخضع تحت الشبكة الواسع ، وهي التي ستقوم بتوصيلنا للفروع الآخر أو في حال نريد الاتصال في شبكة أخرى ولكن في دولة بعيده أيضاً سنخضع تحت اشرف الشبكة الواسعة لأنه هي الشبكة الوحيد التي لا حدود له في المساحة الجغرافية .

- **من ماذا تتكون شبكة الـ WAN** : تتكون الشبكة من أجهزة كثيرة مثل الراوترات السويشتات والسيرفرات ، ولكن كل هذه المعدات والأجهزة تكون ملكية خاصة بشركة الاتصالات .
- تتمثل شبكة الـ WAN مثل شبكة الانترنت الواسعة التي تربط جميع العالم ببعضه البعض ، والتي من خلال شبكة الانترنت تستطيع أن تتصل بشبكة بعيدة مثل في دولة أمريكا وفلسطين وأكبر مثال على هذه الشبكة هو أننا نستطيع الاتصال ببعضنا البعض عن طريق الفيس بوك هذا أكبر مثال على أننا متصلين بشبكة الانترنت والتي تخضع تحت شبكة الـ WAN ، مثل شبكة الفيس بوك غير موجودة في دولة فلسطين ولكن موجودة في دولة أمريكا ولكن كيف لنا أن نتصل في شبكة الفيس بوك ونستطيع التواصل مع بعضنا البعض ، وعن طريق الشبكة الواسعة التي تقوم بتوصيلنا لشبكة الفيس بوك

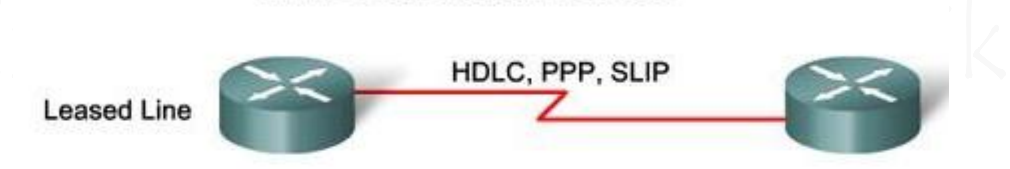
وغيرها من الشبكات الآخر عن طريق تحويل الـ **Packets** من شبكة إلى أخرى حتى تصل للشبكة المستهدفة .

- شبكة الـ **WAN** تعمل مع الطبقة الأولى من طبقة الـ **OSI Layer** و هي الطبقة المادية .
- شبكة الـ **WAN** يوجد لها عدة أنواع من الاتصال مع بعضها البعض سنقوم بذكر هذه الأنواع و شرح كل نوع لوحده لنستطيع فهم الأنواع بشكل مبسط .

- **أنواع اتصال الشبكات الواسعة WAN Connection Types سنقوم بذكرهم وشرحهم بالتفصيل .**

Leased Line, 2- Circuit Switching, 3- Packet Switching

١- **Leased Line** : الخط المؤجر هذا النوع من الاتصال يتم من خلال شركة الاتصالات أو من خلال مزودي خدمة الانترنت **ISP** ، حيث نقوم باستئجار خط **Leased Line** ليكون خاص بالشركة ليربط ما بين الفروع فقط و غير مشترك فيه أحد بمعنى أنه يكون لتوصيل الشبكات الخاصة بالشركة أو المؤسسة مع بعضها البعض .



- **مميزات الـ Leased Line :**

- سريع جداً وذلك لأنه لا يشترك فيه أحد غير الشركة، وتكون سرعة الناقل عالية جداً ومن جهة الأمن والحماية أفضل بكثير من أي أنواع آخرى لأن البيانات والمعلومات تكون في قناة اتصال واحدة ولا أحد يستطيع الاتصال بها .

- من جهة التكلفة مكلف جداً جداً ولذلك لا أحد يستخدمه غير الشركة الكبيرة والضخمة والشبكة التي تعمل ببيانات حساسة وجودة عالية ، مثل شبكة البنوك وشبكة الاتصالات والشبكات الحكومية كل هذه المؤسسات حساسة جداً في نقل البيانات لذلك يفضلو استخدام نوع الـ **Leased Line** أكثر أمان وسريع جداً في نقل البيانات والمعلومات.

- طريق الاتصال والربط عن طريق الـ **Leased Line** تتطلب عدة أمور مثلاً يجب أن يتوفر أجهزة الربط مثل الراوترات والسويتشات ، وأيضاً يعتمد هذا النوع من الاتصال على بعض البروتوكولات التي يجب تفعيلها عندما ا نريد العمل بـ **Leased Line**.

- البروتوكولات التي تعمل مع الـ **Leased Line** نوعان سنقوم بذكرهم وشرحهم بالتفصيل **PPP** , **HDLC** .

- **High Level Data Link Control (HDLC)** : هذا البروتوكول ملكية لشركة سيسكو ومن أقدم البروتوكولات الموجودة في العالم، وهو يستخدم لربط فروع الشبكات ببعضها ليتم الاتصال ما بينهم ويجب أن نعرف أن هذا البروتوكول لا يعمل إلا على راوترات سيسكو فقط ويعمل مع منافذ السيريل ولكن يجب تفعيله ليبدأ في العمل ومع العلم أنه يعمل بشكل تلقائي.

- بروتوكول الـ **HDLC** يقوم بعملية تغليف للبيانات ما قبل عملية الإرسال بخطوط الربط ، وتتم العملية عن طريق إضافة الـ **IP Header** .

- يوجد إصدران من بروتوكول الـ **HDLC** بعد أن قامت شركة سيسكو بتطويره .

١- **HDLC** هذا الإصدار الأول من البروتوكول يحتوي على **6** حقول كما في الجدول التالي.

Standard HDLC					
Flag	Address	Control	Data	FCS	Flag

- Supports only single-protocol environments.

سنقوم بشرح كل من هذه الحقول بالتفصيل بعد أن نتعرف على الإصدار الثاني ونعرف الفرق ما بينهم.

٢- **HDLCv2** هذا الإصدار الثاني من البروتوكول ولكن يحتوي على **7** حقول كما في الجدول التالي، مع العلم انه تم إضافة حقل واحد فقط المسمى **Proprietary** وسنقوم بشرح هذه الحقول.

Cisco HDLC						
Flag	Address	Control	Protocol	Data	FCS	Flag

- Uses a protocol data field to support multiprotocol environments.

Flag: هذا الحقل هو المسؤول عن بداية تكوين الإطار **Frame** وهي التي تبدأ بجمع المعلومات المطلوبة حيث أن المعلومات التي يتم جمعها سيتم استلامها لآخر حقل في الإطار لتكون بنفس المعلومات، وحجم هذا الحقل **8 bits**.

Address : هذا الحقل هو المسؤول عن عنوان الـ **IP** الخاص بجهاز المرسل وجهاز المستقبل حيث يتم وضعهم في حقل واحد، و حجم هذا الحقل **8 bit**.

Control : هذا الحقل من أهم الحقول وهو المسؤول عن إرسال واستلام الرسالة حيث يقوم بعملية تحكم كاملة تسمى الـ **Flow Control**، حيث تقوم ببناء علاقة ما قبل عملية الإرسال والاستقبال وحجم هذا الحقل **8 bit**.

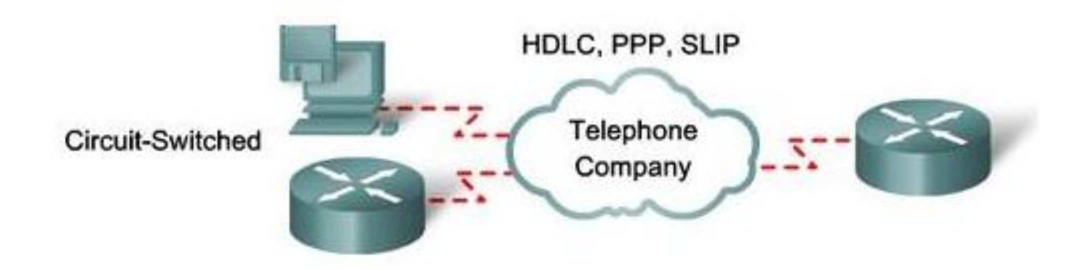
Protocol : هذا الحقل الذي يقرر نوع البروتوكول المستخدم من الممكن أن يكون بروتوكول الـ **PPP, HDLC** وتكوين الـ **LLC Header**.

Data : هذ الحقل المسؤول عن البيانات التي تتغير في كل الاوقات، وفي بعض الحالة يسمى هذا الحقل متغير لأنه البيانات التي تكون في داخله متغيرة وحجم هذا الحقل مفتوح.

FCS : هذا الحقل المسؤول عن عملية التحقق من سلامة الإطار قبل إرساله، حيث عندما يبدأ في عملية التكوين و يتم الوصول إلى حقل الـ **FCS** سيقوم بفصح الإطار قبل إرساله للطرف الآخر ليتاكد هل يوجد خطاء ما في الإطار أو لا اذا لما يجد اية اخطاء سيكمل العملية بشكل طبيعي.

Flag : هذا الحقل المسؤول عن نهاية الإطار فهو يأتي في آخر عملية التكوين، وعندوصول الإطار لهذا الحقل سيتم معاودة النظر على المعلومات التي تم تكوينها من البدايةحتىوصول الإطار لهذا الحقل وقبل إرسال البيانات أو الإطار سيتم النظر عليها وبعدها سيتم معاودة إرساله للشبكة المطلوبة.

٢- **Circuit Switching** تبديل الدوائر ما بين الشبكات وعند استخدام **Circuit-Switching** لنقل البيانات فإن على الجهازين المرسل والمستقبل أن يكونا متفرغين لنقل البيانات بينهما فقط، ثم يتم إنشاء تتابع مؤقت من الدوائر من نقطة إلى آخرى بين الجهازين ويتم الربط بين هذه الدوائر معاً باستخدام مفاتيح تبديل، ويتم تحقيق الإتصال فور الإنتهاء من فترة صغيرة للإعداد، وتكون سرعة النقل بين الجهازين ثابتة.



- **خصائص الـ Circuit Switching :**

١- التكلفة العكسية **Reverse Charging** مثل قيمة المكالمة تستقر على طرف من الطرفين، عندما ا يتم فتح اتصال أول خط من الطرف المراد يبدأ العد عليه بحسب التكلفة عليه.

٢- من مميزات هذا النوع من الاتصال والربط أنه يقوم بتحويل المكالمة **Call Redirect**.

٣- يتم ربط الاتصال فقط عندما ا نريد الاتصال مثل الهاتف عندما ا نريد الاتصال بأحد نقوم برفع سماعة الهاتف، و نسمع أنه يوجد صوت حراره هذا يدل على أننا نستطيع الاتصال ولكن عندما ا تغلق سماعة الهاتف لن نستطيع الاتصال لأنه تم اقفال المسار .

- **عيوب نظام الـ Circuit Switching :**

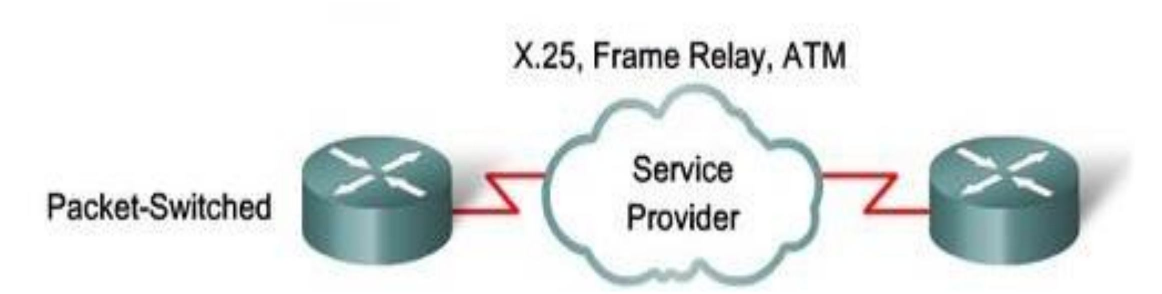
١- عند زيادة حركة المرور في داخل الشبكة سيتم انخفاض معدل السرعة الخاص بنقل البيانات .

٢- في حال تريد إرسال بيانات أو تريد الاتصال في حاسوب ما و كان هذا الحاسوب مشغول سيقوم بانتظار الحاسوب لينتهي من الخط الذي يعمل فيه وبعدها يسطيع الاتصال به، مثلاً عندما ا نتصل بأحد من الجوال أو الهاتف ويكون هذا الشخص مشغول باتصال آخر ونحن نقوم بالاتصال به لن تستطيع التكلم معه لأن الخط مشغول مع شبكة أخرى في هذه الحالة علينا الانتظار بينما ينتهي من المكالمة والتي كون مفتوحه في الخط وبعدها نستطيع الاتصال به و التكلم معه .

٣- العيب الأكبر لهذا النظام انه فقط يقوم بإنشاء مسار واحد ما بين الجهازين فقط مهما كان حجم هذه البيانات ، فقط سيقوم بإنشاء خط واحد والعمل من خلاله ولو كان جهاز ثاني يريد الاتصال بأحد الأجهزة لا يستطيع إلا بعد أن يقفل أحد الأجهزة الخط المتصل فيه ليستطيع الاتصال به .

٤- في عملية الاتصال في هذا النظام يجب على الجهازين أن يستخدمون نفس البروتوكول ما بينهم ليتم الاتصال .

٣- **Packet Switching :** يعد هذا النوع من أسرع التقنيات التي ذكرناها وهو الأساسي لمعظم شبكات الاتصالات حتى في الوقت هذا نعمل بهذا النظام، وفي هذا النظام عملية الإرسال تكون مختلفة عن عملية الإرسال في التقنية السابقة، في هذا النظام لا ترسل الرسالة بشكل كامل مرة واحدة بل يتم تقسيمها إلى عدة حزم صغيرة ويتم إرسالها إلى الجهاز المستهدف، حيث يقوم جهاز المستقبل بإعادة تكوينها مرة أخرى للرسالة الأصلية ويقوم بإضافة العناوين كل من عنوان جهاز المرسل وجهاز المستقبل وباقي المعلومات المطلوبة للتحكم.



يعتمد هذا النظام في عملية الربط والتوصيل على كوابل الـ **Serial** ليربط ما بين أجهزة التوصيل ويسمى الطرف المرسل **Data Communication Equipment(DCE)**

حيث أنه يقوم بإرسال حزم البيانات بشكل مقطع ومقسم إلى عدة حزم صغيرة ويقوم بإرساله بشكل مفصل عن بعضها البعض مثل حزم تسلك مسار آخر وحزم تصل ما قبل الحزم الآخر

وكل من هذه الحزم تسلك طريق ولكن عند وصول الحزم إلى الهدف المطلوب سيتم معاودة تجميع كل الحزم لتتكون في حزمة واحدة وتسليهما للجهاز المطلوب بشكل كامل.

- **مميزات Packet Switching :**

١- لا يشترط على المرسل والمستقبل أن تكون السرعة حيث يستطيع الجهازين العمل بسرعة مختلفة ، ولا يشترط أن يعملوا بنفس البروتوكولات مثل التقنية السابقة .

٢- في أوقات إرسال الحزم في المسارات لا يستغرق وقت كبير ، لأنه حجم الحزمة صغير و يتم إرسالها بشكل سريع جداً بهذا الشكل المسار لن يبقى مشغول لفترة طويله.

٣- من جهة المشاكل وقوع بعض الحزم في هذا النظام في حال وقوع أحد الحزم أو عدم وصولها بشكل كامل سيتم معاودة إرسالها مرة أخرى بشكل طبيعي وسريع وذلك لأن حجم الحزمة صغير.

- يوجد بعض المعلومات يجب أن نكون على معرفة بها قبل أن نبدأ العمل بهذا النظام لنتعرف على هذه المعلومات ليتم العمل بشكل صحيح.

١- يجب الاتفاق على حجم تقسيم الرسالة المرسلة التي يتم تقسيمها إلى حزم صغيرة.
٢- يجب الاتفاق على المسارات التي سيتم الإرسال والاستقبال منها حزم البيانات.
٣- يجب معرفة معلومات التحكم بعملية تدفق البيانات ومعالجة الأخطاء.

- قبل أن نتعمق أكثر في موضوع الشبكة الواسعة يجب أن نتعرف على بعض البروتوكولات المهمة جداً جداً في عملية الربط والاتصال .

X.25 : هو البروتوكول أو المعيار الذي ينظم تدفق البيانات في الشبكات **Packet-Switching** وهو يمثل الواجهة ما بين **Data Communication Equipment** (**DCE**) والتي سبق أن قمنا بشرحها، وبين **Data Terminal Equipment** (**DTE**) والتي تمثل أجهزة كمبيوتر المتوافقة مع بروتوكول **X.25** وقد تكون عبارة عن موجه **Router** أو بوابة **Gy** .

مكنونات بروتوكول **X.25** حيث يتكون هذا البروتوكول من عدة طبقات التي تندرج تحت طبقات الـ **OSI Layers** سنقوم بذكرهم والتعرف عليهم :

١- يعمل مع الطبقة الأولى وهي الطبقة الفيزيائية **Physical Layer** هذه الطبقة تعتبر الطبقة المادية لأنه تعمل مع الكوابل وكروت الشبكة.
٢- يعمل مع الطبقة الثانية وهي طبقة ربط البيانات **Data-Link Layer** وهي التي تعمل على ربط البيانات في خصائصها مثل معرفة البروتوكول المستخدم وربط البيانات فيه.

٣- يعمل أيضاً مع الطبقة الثالثة و هي طبقة الشبكة و هي المسؤولة عن الشبكة وتحويل ما بين الشبكات و هذه الطبقة التي تعمل فيه الـ **Packets** .

الآن لنفهم لماذا يتم استخدام هذه الطبقة في هذا البروتوكول :

- الطبقة الأولى تقوم بتوفير الأصفار و الوحايد المتسلسلة مع توفير نوع الاتصال المزدوج الـ **Full Duplex** ، وتعمل هذه الطبقة بشكل مباشر مع الكابل حيث تتحكم في البيانات وتنتقل إلى الهدف المطلوب عبر الشبكة .

- الطبقة الثانية تقوم بتوفير الوقت و الزمن المطلوب للبيانات المرسلة، و تقوم بالتأكد من فراغ إطارات حيث تكون البيانات على شكل حزم في الطبقة الشبكية ثم تتحول إلى إطارات في الطبقة الثانية ، و تقوم أيضاً بالتحكم بتدفق الإطارات التي ما بين الـ **DCE , DTE** و البروتوكول المستخدم في هذه الطبقة من عائلة الـ **X.25** هو بروتوكول الـ **HDLC**.

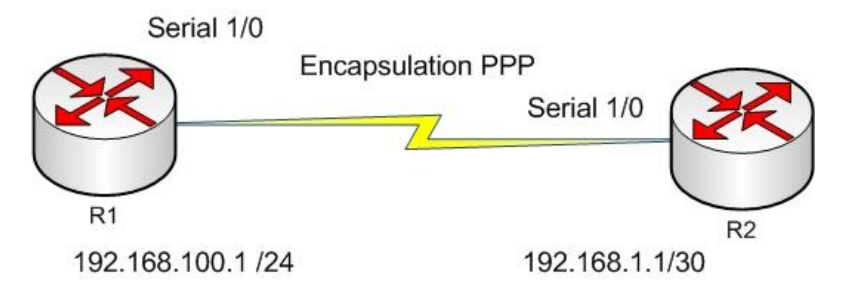
- الطبقة الثالثة و هي التي تقوم بعمل إعداد الدوائر الظاهرية ما بين الاجهزة المتصلة ، وتقوم أيضاً بتقسيم البيانات إلى عدة حزم صغيرة ، وتكون على معرفة بعنوان وتوجيه البيانات ما بين الأجهزة في الشبكة، وتقوم بعملية معالجة الأخطاء التي حصلت أثناء عملية الإرسال .

نهاية الموضوع يعتبر بروتوكول الـ **X.25** هو البروتوكول أو المعيار الذي يقوم بتنظيم تدفق البيانات عبر شبكات الـ **Packet-Switching** وينقسم إلى ثلاث طبقات من طبقة الـ **OSI Layers** .

Physical Layer, Data-Link Layer, Network Layer

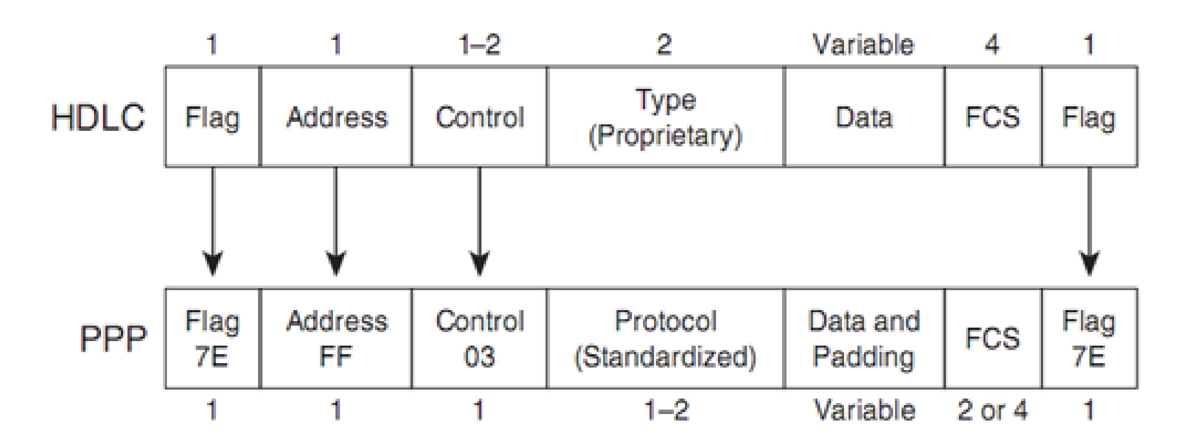
Point to Point Protocol (PPP)

بروتوكول النقطة للنقطة



PPP : هو من أهم البروتوكولات الخاصة بربط وتوصيل الشبكات الواسعة **WAN**، حيث يعمل هذا البروتوكول في الطبقة الثالثة **Data Link** من طبقة الـ **OSI Layers** ، وهذا البروتوكول ليسه ملكية بشركة سيسكو على العكس بروتوكول الـ **HDLC** الذي ينتمي لشركة سيسكو ومع العلم أنه لا يتفوق على بروتوكول الـ **PPP** حيث هذا البروتوكول لديه المميزات والخصائص تتفوق بكثير على بروتوكول الـ **HDLC**.

- يتكون بروتوكول الـ **PPP** من **Header** وهو نفس الـ **Header** الذي قمنا بشرحه مسبقاً في بروتوكول الـ **HDLC** كما هو موجود في الجدول التالي .



ولكن يجب أن نعلم هذا لا يعني انه الـ **Header** الموجود في بروتوكول الـ **HDLC** يعمل بنفس وظيفة الـ **Header** الموجود في بروتوكول الـ **PPP** ، الأسماء تشبه بعضها البعض ولكن يوجد بعض الوظائف التي تعمل في بروتوكول الـ **HDLC** وبعض الوظائف لا تعمل في بروتوكول الـ **PPP** سنتعرف على هذا الفرق في الجدول التالي، ولكن قبل أن نبدأ بالتعرف على المميزات الموجودة في **Header** الـ **HDLC** والمميزات الموجودة في **Header** الـ **PPP** **يجب علينا أن تقوم بمراجعة الـ Header** الذي قمنا بشرحه وشرح الحقول في الدروس السابقة ، لنستطيع أن نفهم ما هو موجود في الجدول التالي :

Feature	HDLC	PPP
Error detection	Yes	Yes
Error recovery	No	Yes
Standard Protocol Type field	No	Yes
Default on IOS Serial links	Yes	No
Supports synchronous and as asynchronous links	No	Yes

- هذه هي المكونات والخصائص التي تعمل في بروتوكول الـ **PPP** و **HDLC**.

- **يتم تقسيم بروتوكول الـ PPP إلى قسمين سنقوم بذكرهم و شرحهم .**

١- القسم الأول وهو الخاص بتحكم في الشبكة **Network Control Protocol** , (**NCP**) و هذا البروتوكول يقوم بعملية الـ **Encapsulation** ما بين الشبكات التي تعمل ببروتوكول الـ **PPP** ويقوم أيضاً بعملية إدارة البروتوكولات التي تعمل في الطبقة الثالثة **Network Layers** مثل بروتوكولات الـ **Apple Talk** , **IPx** , **IP** و غيرها من البروتوكولات الآخر .

٢- القسم الثاني و هو الخاص بالتحكم بالوصول **Link Control Protocol** (**LCP**) هذا البروتوكول هو المسؤول عن عملية تأمين الإتصال ما بين شبكتين تعملان ببروتوكول الـ **PPP** حيث تتم هذه العملية بعد عدة خطوات سنقوم بذكرهم والتعرف عليهم لنعرف كيف تتم عملية التحكم والاتصال ما بين الشبكات التي تعمل من خلال الـ **PPP** .

١- يقوم بعملية التفاوض ما بين الشبكتين **Negotiation** ، وهذه العملية هي المسؤولة عن التأكد من أن حالة الربط صحيحه أم لا و هل جميع الإعدادات صحيحه .

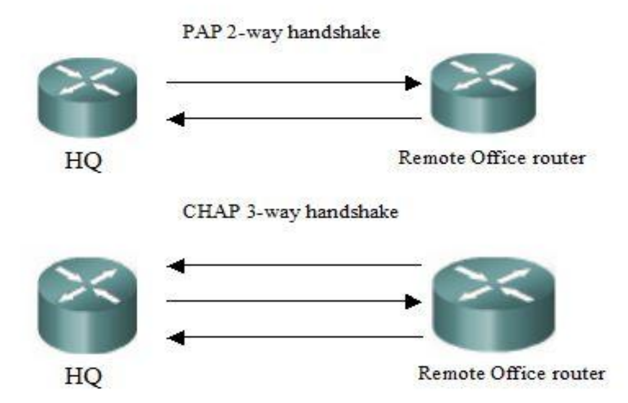
٢- يقوم بعملية تحقق **Authentication** وظيفة هذه العملية التأكد من صحة البيانات والحماية والمعلومات هل هي صحيح ما بين الشبكتين أم لا ، لتقوم بعملية الإرسال .

٣- يقوم بعملية ضغط للبيانات **Compression** في هذه الحالة تقوم الشبكات بالتفاوض ما بين بعضهم البعض ، ليتم الاتفاق على البيانات التي سيتم إرسالها ما بين الشبكات .

٤- عملية الكشف عن الأخطاء **Error Detections** في حال وجد خطأ ما يتم الكشف عنه قبل عملية الإرسال ، ووظيفة هذه العملية أناء تقوم بفحص الـ **Header** بشكل كامل قبل عملية إرساله وفي حال وجد خطأ معين سيتم معاودة طلب البيانات التي يتواجد فيها الخطأ مرة أخرى لتتم عملية البناء من جديد وإرساله مرة أخرى للشبكة .

٥- عملية الوصولات المتعددة في الشبكة **Multilink**، وظيفة هذه العملية في حالة تم وجود عدة مسارات تربط ما بين الشبكتين حيث يتم توزيع الترافيك على المسارات .

PPP Authentication Methods
طرق التحقق من البيانات ما بين الشبكات التي تعمل ببروتوكول الـ PPP



- عندما ا نقوم بعملية الربط والاتصال ما بين الشبكات عن طريق بروتوكول الـ **PPP** من الطبيعي جداً أنه سيتم تبادل المعلومات ما بين الراوترات، لتسطيع الشبكات أن تتصل ببعضها البعض ولكن يجب أن يكون هناك مفتاح أمن يحمي الشبكات من الاختراق ويزيد من أمن الشبكة في عملية تنقل المعلومات ، و يجب أن نعلم أنه في حال لم تتطابق معلومات الـ **Authentication** لن يحصل أي اتصال أو تبادل معلومات ما بين الراوترات إلا إذا تم التطابق سيتم تبادل المعلومات والعمل بشكل طبيعي .

- تتم عملية التحقق الـ **Authentication** عن طريق البروتوكولات التالية :

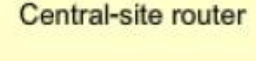
١- Password Authentication Protocol (PAP)

تتم عملية التحقيق من خلال إعدادات يجب أن نقوم نحن بعمل هذه الاعدادات ، يجب أن نقوم بإنشاء مستخدم وكلمة مرور **User Name and Passowrd** ، و يجب أن نعلم أن هذه الإعدادات يتم دمجها في عملية التحقق **Authentication** ، مثال على ذلك عندما نقوم بتركيب راوتران راوتر في شبكة وراوتر في شبكة أخرى ويربطبينهما بروتوكول الـ **PPP** ونريد من الراوتران تتبادل المعلومات من الطبيعي سيقوم أحدهما بطلب المعلومات من الراوتر المجاور له، سيقوم بالرد عليه بعملية الـ **Authentication** وهي عملية التحقق يقول له ادخل البيانات التالية وهي المستخدم و كلمة مرور **User Name and Passowrd** ، وبعدها سيتم التحقق إذا كانت هذه المعلومات صحيح سيتم تبادل المعلومات الداخلية ما بين الراوتران لأنه تم التحقق من هوية الراوتر الأول الذي قام بطلب معلومات الراوتر الثاني .

ملاحظة مهمة جداً : يجب أن نعلم أنه في عملية التأكيد من خلال اسم المستخدم وكلمة المرور يتم نقلها أو كتابتها بشكل ظاهر **Clear Text** وغير مشفر .

٢- Challenge Handshake Authentication Protocol (CHAP)

هذا النوع الثاني من عملية تحقق المعلومات ما قبل عملية الإرسال ولكن هذا النوع وظيفته، عندما ا يريد الراوتر المطلوب تبادل المعلومات هو الذي يبدأ بإرسال طلب للراوتر الثاني لمعرفة المعلومات مثل اسم المستخدم وكلمة المرور **User Name and Passowrd** بمعنى أنه لا ينتظر الراوتر بالتعريف عن نفسه ، ويجب أن نعلم أن النوع الأول يرسل البيانات بشكل مرئي وغير مشفر على عكس النوع هذا الذي يقوم بعملية التشفير أثناء طلب المعلومات مثل الـ **User Name and Passowrd** ، حيث يقوم بتشفيره بنظام التشفير الـ **MD5** .











- كما نلاحظ في النموذج، النوع الأول يقوم بعملية التحقق بإرسال طلب أول محمل بالمعلومات من الرسالة لعملية التحقق وطلب ثاني تأكيد على استلام المعلومات ، بينما النوع الثاني يقوم بإرسال ثلاث طلبات من الرسالة لعملية التحقق ويقوم بعملية التأكد على استلام الطلب وتبادل المعلومات .

- **سنتعرف الآن على إعدادات الـ Leased Line Configuration :**

Leased Line Configuration
إعدادات الخط المؤجر

Router > **enable**

Router # **config t**

Router (config) # **hostname R1**

Router (config) # **interface Serial 1/0**

Router (config-if) # **ip address 223.255.255.254 255.255.255.0**

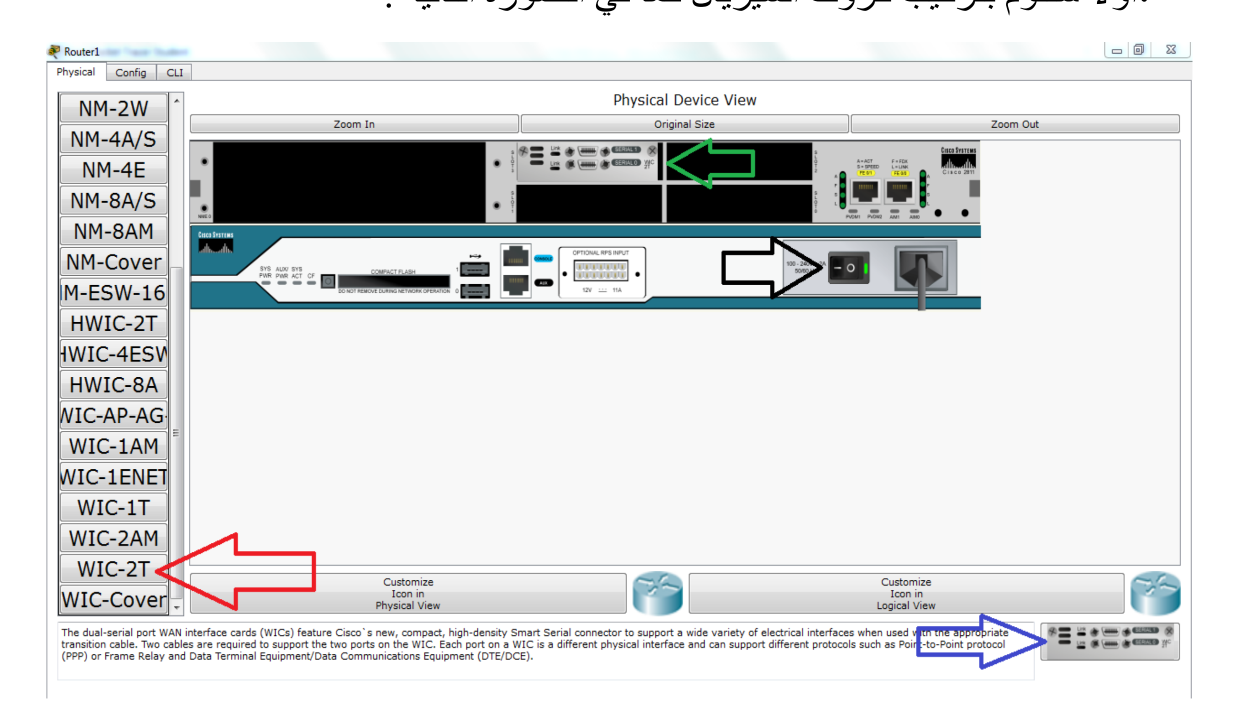
Router (config-if) # **encapsulation ppp**

Router (config-if) # **ppp authentication chap or pap**

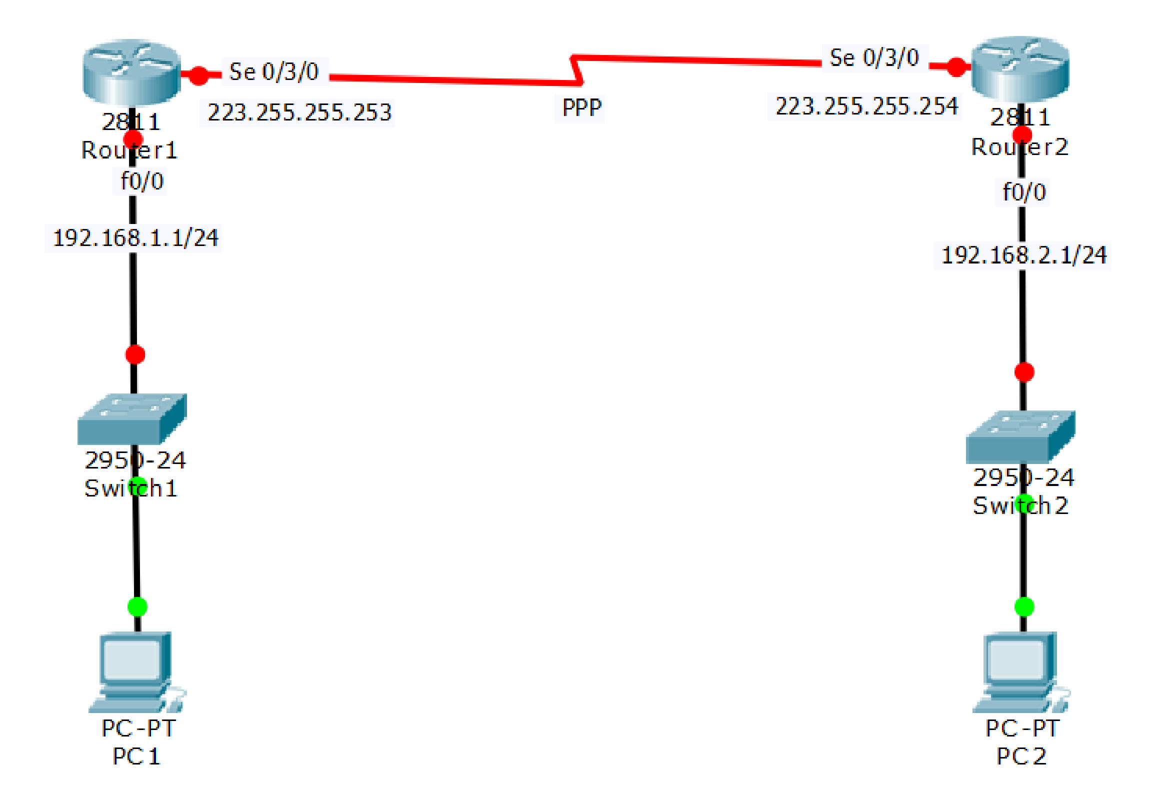
Router (config-if) # **exit**

Router (config) # **username R2 Password cisco123**

- بعد أن تعرفنا على الإعدادات سنقوم بالتطبيق بشكل عملي على شبكة مكونة من راوترين ، ويربط ما بينهم بكابل سيريل **Serial Cable** وسنقوم بتفعيل بروتوكول الـ **ppp** ولكن قبل أن نبدأ بعملية إعدادات للراوترات يجب أن نقوم بتركيب كروت السيريال على الراوترات لنقوم بربطهم ببعضهم البعض وبعدها سنقوم بعملية الإعدادات أولاً سنقوم بتركيب كروت السيريال كما في الصورة التالية :



- كما نلاحظ في الصورة السابقة سنقوم بالدخول على إعدادات الراوتر و سنقوم بايقاف تشغيل جهاز الراوتر لنستطيع إضافة كرت السيريال ،الآن بعد أن قمنا بإيقاف تشغيل الراوتر سنقوم بالذهاب لسحب كرت السريال والذي يشير به بسهم الاحمر وسيظهر النوع المطلوب أسفل مثل الذي يشير عليه السهم الأزرق ، سنقوم بسحب الكرت ووضعه مكان ما هو مشار اليه السهم الأخضر بهذا الشكل نكون قد قمنا بإضافة كرت السيريال بنجاح، ولكن لا ننسى أن نقوم بتشغيل الراوتر قبل الخروج ، ولا ننسى أن نقوم بنفس الطريقة على الراوتر الثاني .
- الآن سنقوم بربط ما بين الراوترات عن طريق كوابل السيريال كما في النموذج التالي هو الذي سنقوم بالتطبيق عليه بشكل عملي .



- هذا هو النموذج والشبكة واضحة ولكن يجب أن نعلم أن الشبكة التي سترتبط ما بين الشبكتين هي الشبكة التي بعنوان **223.255.255.0** وسيتم تفعيل بروتوكول الـ **ppp** على الراوترين ليتم تبادل المعلومات .

- سنقوم الآن بالتطبيق العملي على الشبكة، وسنقوم بالدخول على الراوتر الأول **R1** ونقوم بكتابة الإعدادات التالية :

Router > **enable**

Router # **config t**

Router (config) # **hostname R1**

Router (config) # **interface Serial 0/3/0**

Router (config-if) # **ip address 223.255.255.253 255.255.255.0**

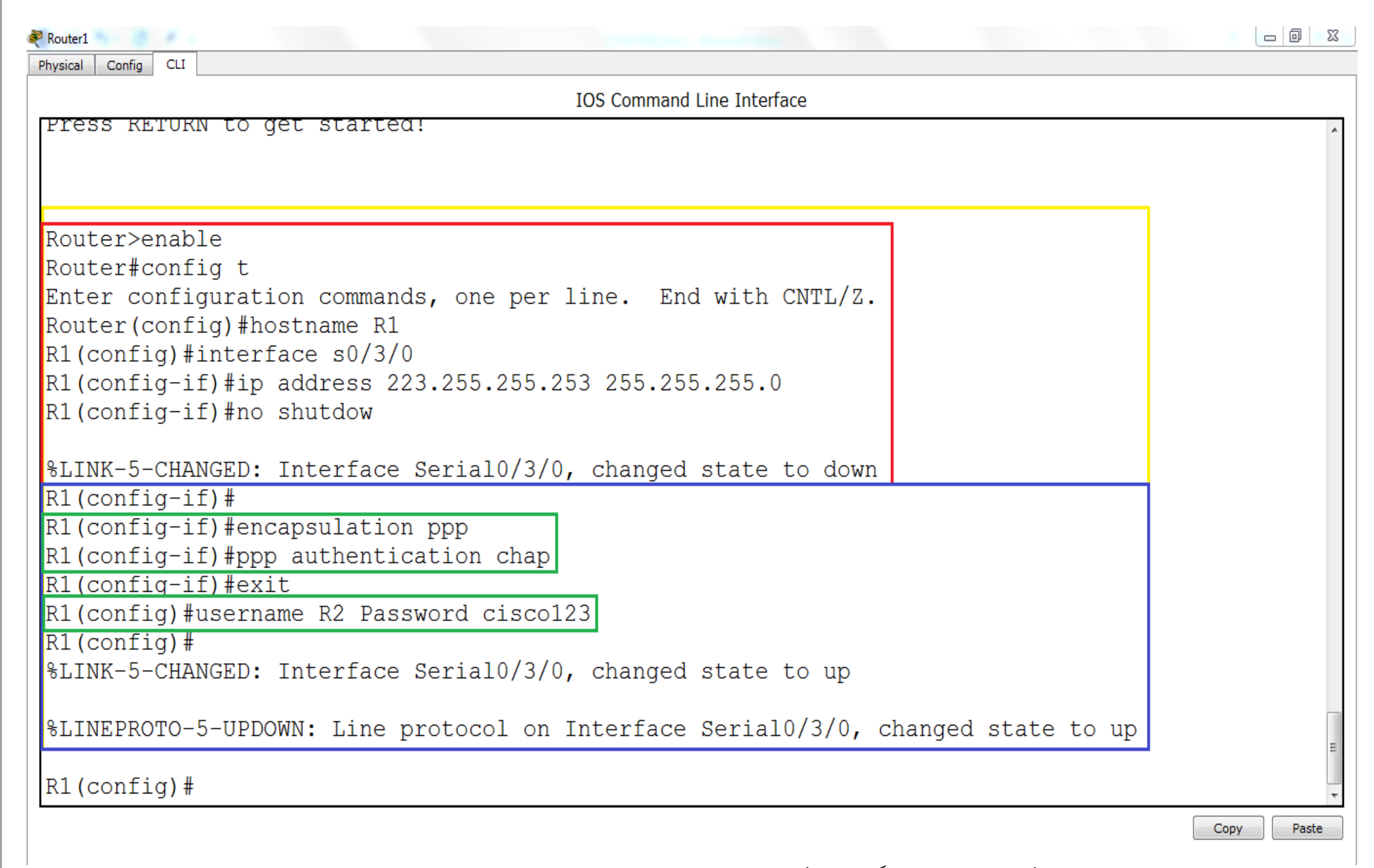
Router (config-if) # **encapsulation ppp**

Router (config-if) # **ppp authentication chap**

Router (config-if) # **exit**

Router (config) # **username R2 Password cisco123**

كما في الصورة التالية من داخل الراوتر الأول **R1**



- ولا ننسى الأمر المهم جداً و هو أمر حفظ الإعدادات كما في الصورة التالية :

R1 # **copy running-config startup-config**

```
R1#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
R1#
```

- بهذا الشكل يكون قد تم الانتهاء من إعدادات الراوتر الأول **R1** وسنقوم بدخول على الراوتر الثاني **R2** و سنقوم بعمل الإعدادات التالية:

- سنقوم الآن بالدخول على الراوتر الثاني **R2** ونقوم بكتابة الإعدادات التالية :

Router > **enable**

Router # **config t**

Router (config) # **hostname R2**

Router (config) # **interface Serial 0/3/0**

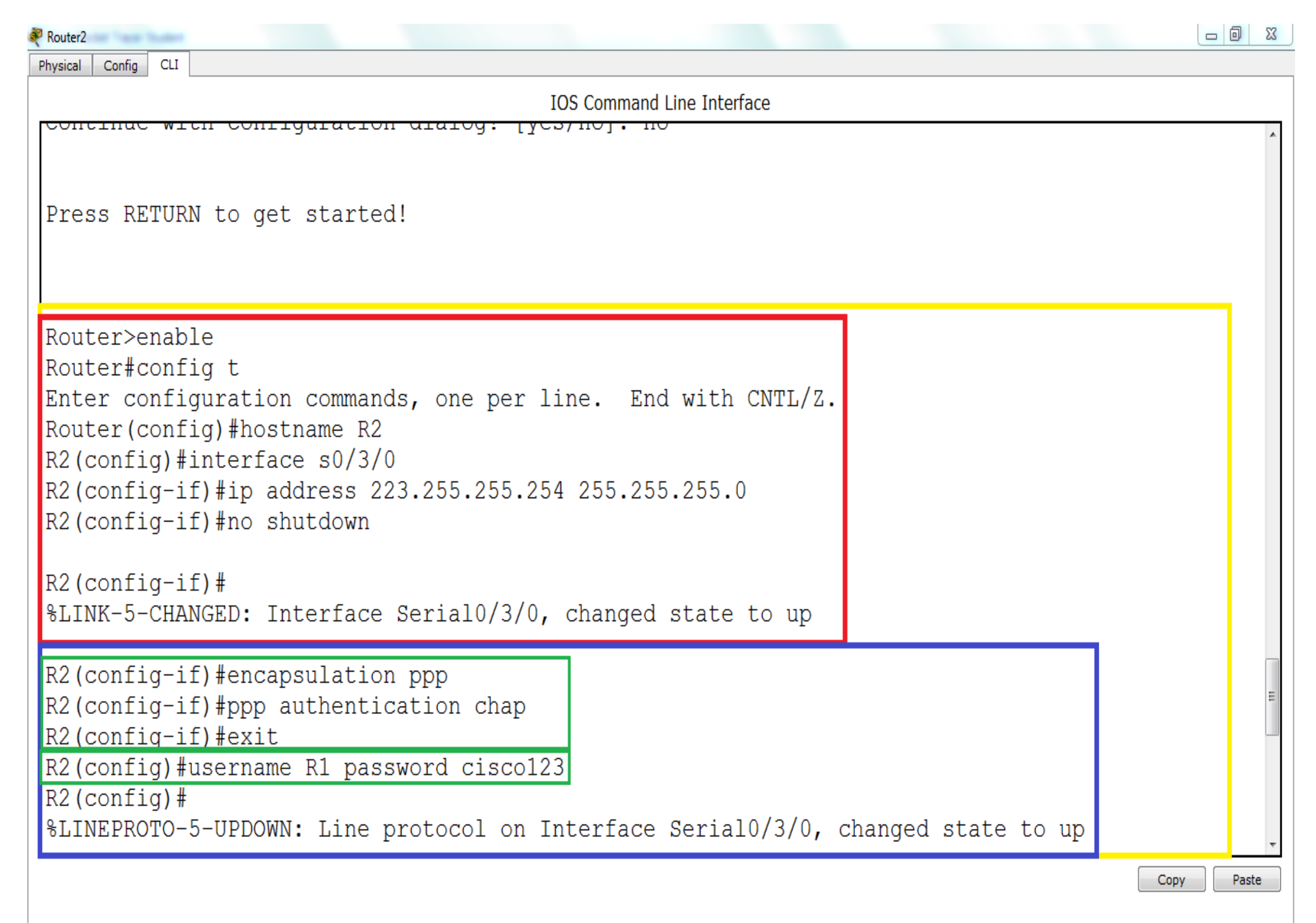
Router (config-if) # **ip address 223.255.255.254 255.255.255.0**

Router (config-if) # **encapsulation ppp**

Router (config-if) # **ppp authentication chap**

Router (config-if) # **exit**

Router (config) # **username R1 Password cisco123**

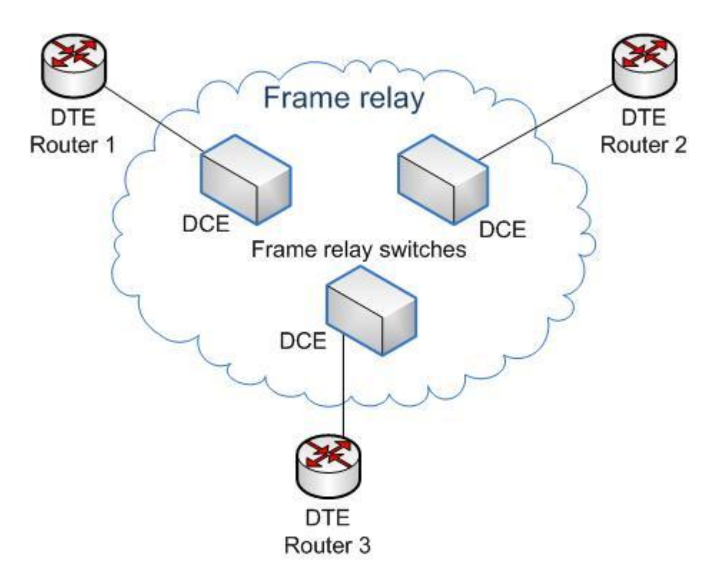


- ولا ننسى الأمر المهم جداً وهو أمر حفظ الإعدادات كما في الصورة التالية :

R2 # **copy running-config startup-config**

Frame Relay Protocol

بروتوكول ترحيل اطر المعلومات



Frame Relay: هي تقنية من تقنيات تبادل الحزم مثل الـ **Packet Switching**، وهي التقنية التي قمنا بالتكلم عنها في الدروس السابقة وتعمل هذه التقنية على عملية الربط بشكل سريع وسهل لأن البيانات التي يتم إرسالها في الشبكة تكون على شكل حزمة تسمى هذه الحزمة إطار **Frame** ، وتتميز هذه التقنية بالمرونة والسرعة العالية في عملية الاتصال ما بين الشبكات وتكون ذات وثوقية عالية جداً وتتراوح سرعة النقل في هذه التقنية ما بين **56 kbps** و **45 kbps** , وتعد هذه التقنية من التقنيات ذات الفعالية الكبيرة جداً نظراً لقدرتها على التحكم بتدفق البيانات وإضافة إلى أنها ذات آلية بسيطة جداً لتوجيه البيانات في الشبكات.

أهم الوظائف التي تعمل فيها تقنية الـ Frame Relay :

١- الاتصال ذات السرعة العالية جداً جداً في عملية الإرسال والاستقبال .
٢- تكون عملية الاتصال ما بين الشبكات موثوقة جداً .
٣- يتم تبادل الحزم عن طريق بروتوكول الـ **X.25**.
٤- المسؤول عن تحديد معيارات هذه التقنية هي هيئات **ANSI** و **CCITT/ITU** بالإضافة إلى منتدى **Frame Relay Forum** و هو عبارة عن منتدى أبحاث يجمع بين منتجي و مزودي تقنية **Frame Relay** .
٥- الوظيفة الأساسية لهذه التقنية هي عملية توفير سرعة عالية جداً تربط ما بين الشبكات المحلية لتكوين الشبكة الواسعة **WAN**.
٦- تعمل هذه التقنية بوظيفة خدمة الموجه الـ **Connection-Oriented**، وتتم هذه الوظيفة على عمل إعدادات دائرة ظاهرية دائمة **Permanent Virtual (PVC) Circuit** لتقوم بربط ما بين أجهزة المرسل وأجهزة المستقبل .
٧- يتم تحديد **PVC** عن طريق المسار الذي سيتم إرسال البيانات منه من جهاز المرسل إلى جهاز المستقبل من شبكة الـ **Frame Relay**.

مميزات تقنية الـ Frame Relay :

١- إرسال البيانات بشكل مبسط لتوجيه البيانات بمعن المسارات تكون واضحه.
٢- تحتوي هذه التقنية على نظام التحكم بالبيانات المتدفقة من الطرفين.
٣- لا تحتاج نظام التحقق من أخطاء البيانات والمعالجة .
٤- هذه التقنية توفر لنا خيارات أسرع بكثير من تقنية أو شبكة الـ **ISDN** والخطوط المستأجرة .
٥- تقوم بعملية النقل على مختلف أنواع الإشارات .
٦- تقوم بالتوزيع التلقائي على النطاقات الموجودة داخلها .

خطوات إضافة الشبكات في داخل تقنية الـ Frame Relay :

١- يتم إضافة الشبكات عن طريق مزود الخدمة وهو من يقوم بإدارة الشبكة .
٢- يقوم مزود الخدمة بتركيب عناوين الـ **DLCI** وهو رقم الراوتر الموجود في الدائرة الوهمية الافتراضية ، في حال تم استخدام تقنية الـ **Frame Relay** .
٣- عندما ا يقوم أحد الأجهزة بإرسال بيانات سيتم تحويله لشبكة الـ **Frame Relay** وفي داخل الشبكة سيتم تحديد الدائرة الظاهرية التي تكلمنا عنها مسبقاً **PVC** وهي المسؤولة عن نقل البيانات للجهاز أو الشبكة المطلوبة .
٤- سيتم إضافة عناوين الأجهزة المستهدفة مثلاً سيتم إضافة عنوان جهاز المرسل وجهاز المستقبل في كل إطار **Frame** سيتم إرساله.

٥- عندما ا تصل الإطارات إلى نقطة التحويل أو التبديل **Switch** ، سيقوم أولاًال بنظر على عنوان الـ **DLCI** وسيتم معرفته ليعرف من هو الجهاز المستقبل ومن هو الجهاز المرسل وأي مسار سيتم سلكه وبعدها سيتم إرسال أو توجيه الإطار للشبكة المطلوبة .

٦- تسلك الإطارات نفس المسار بين المرسل والمستقبل بنفس التتابع مما يعني أنه ليست هناك أي قرارات توجيه مناطة بنقاط التبديل فالمسار يرسم ويعد قبل الإرسال وبالتالي ليست هناك أي مشكلة بخصوص تتابع البيانات المستقبلة ولكن ينتج عما سبق عيب واضح لهذه التقنية وهو أنه في حال إزدحام أحد المسارات على الشبكة ليس هناك أي طريقة لإعادة توجيه البيانات إلى مسارات غير مزدحمة ، ولحل هذه المشكلة تستخدم هذه التقنية آلية تسمى **In-Band Congestion Signaling** حيث تقوم الشبكة عندما ا تعاني من ازدحام بتوجيه تحذيرات إلى الأجهزة المرسلة تعلمها بالمسارات التي تعاني من ازدحام لكي يتم تفاديها إذا وصلت الشبكة إلى مرحلة الإشباع فإنها تقوم بالتخلص من الإطارات التي لا تستطيع نقلها أو التي تكتشف أنها معطوبة، وعند وصول الإطارات إلى الكمبيوتر المستقبل سيكتشف من تتابع الإطارات أن هناك بعض الإطارات المفقودة عندها يقوم الجهاز المستقبل بالطلب من الجهاز المرسل أن يعيد إرسال الإطارات التي تم التخلص منها أثناء الإزدحام الشديد للشبكة، نلاحظ مما سبق أن الأجهزة هي المسؤولة عن معالجة الأخطاء وليس الشبكة مما يخفف العبء عن الشبكة ويحسن أداءها .

كيفية التخلص من الإطار في داخل شبكة الـ Frame Relay:

١- يتم التخلص من الإطار في تم وجود أخطاء في الإطار أو مشاكل سيتم إلغاء هذا الإطار من الشبكة ولن يتم إرساله أو استقباله.
٢- يتم أيضاً التخلص من الإطار في حال أن حجم الإطار أكبر من الحجم الطبيعي.
٣- يتم إلغاء الإطار في حالة تم اكتشاف أن البيانات المرسلة أكبر مما هو متفق عليه وفي هذه الحالة سينتج اختناق في الشبكة وازدحام كبير.

شبكة الـ Frame Relay يوجد منه قسمين:

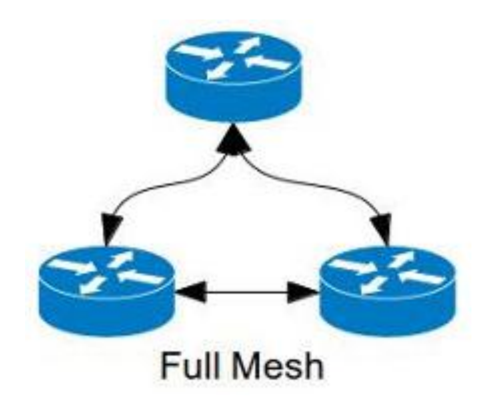
١- القسم الأول شبكة واسعة وكبيرة جداً وتكون هذه الشبكة بشكل عام للجميع ، وهذه الشبكة تكون تحت إشراف شركة الاتصالات أو شركة مزودي خدمة الانترنت فعندما ا تريد شركة معينة الاشتراك بخط معين لتقوم بتوصيل في الشبكة الآخر سيتم هذا الموضوع من خلال شركة مزودي الخدمة أو شركة الاتصالات ولتتم هذه العملية هناك بعض الاشياء التي يجب أن يتحقق منه ويجب أن يعلم بها المشترك في الخط مثل **Customer Termination Equipment (CTE)** سنقوم بشرحها أسفل، **PVC** رقمي مستأجر, نقطة خدمة **Frame Relay Service Point .**
٢- القسم الثاني شبكة واسعة وكبيرة جداً ولكن خاصة مثل تكون ملكية لشركة أو مؤسسة.

CTE: هو الجهاز الذي يقوم بعملية الربط ما بين المشرك وشبكة الـ **Frame Relay** ، و يكون هذا الجهاز راوتر أو جسر ناقل.

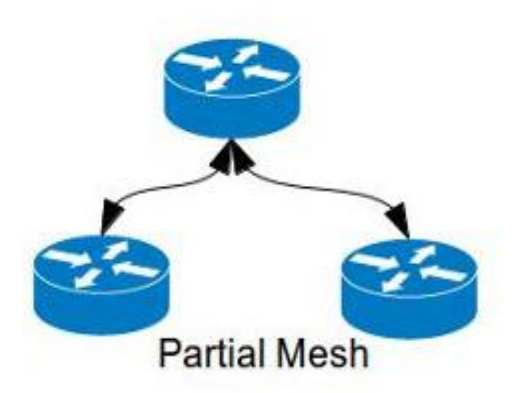
لنستطيع فهم و توضيح هذه التقنية و أهمية استخدامها، لنفترض أن لدينا شركة لها أربعة فروع في أماكن متباعدة، لربط هذه الفروع معاً ومع المركز الرئيسي دون استخدام تقنية **Frame Relay** فإنه سيلزمنا استئجار عشرة خطوط للربط بين جميع الفروع معا أما باستخدام **Frame Relay** فكل ما نحتاجه هو استئجار خط قصير لربط كل فرع بأقرب مزود لخدمة **Frame Relay** .

يوجد أكثر من شكل لربط الشبكات من خلال تقنية الـ Frame Relay :

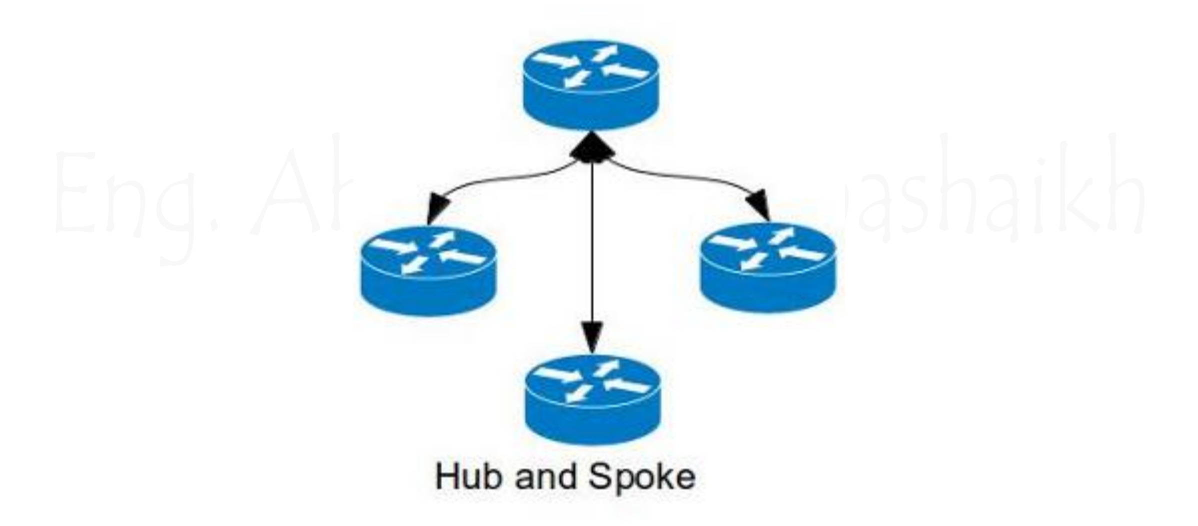
١- الربط الكامل والذي يمثل ربط الشبكة بشكل كامل وغير متقطع أو منفصل **Full Mesh .**



٢- الربط المجزأ و هو يمثل الربط المتقطع على عكس الربط الكامل **Partial Mesh** **Topology**.



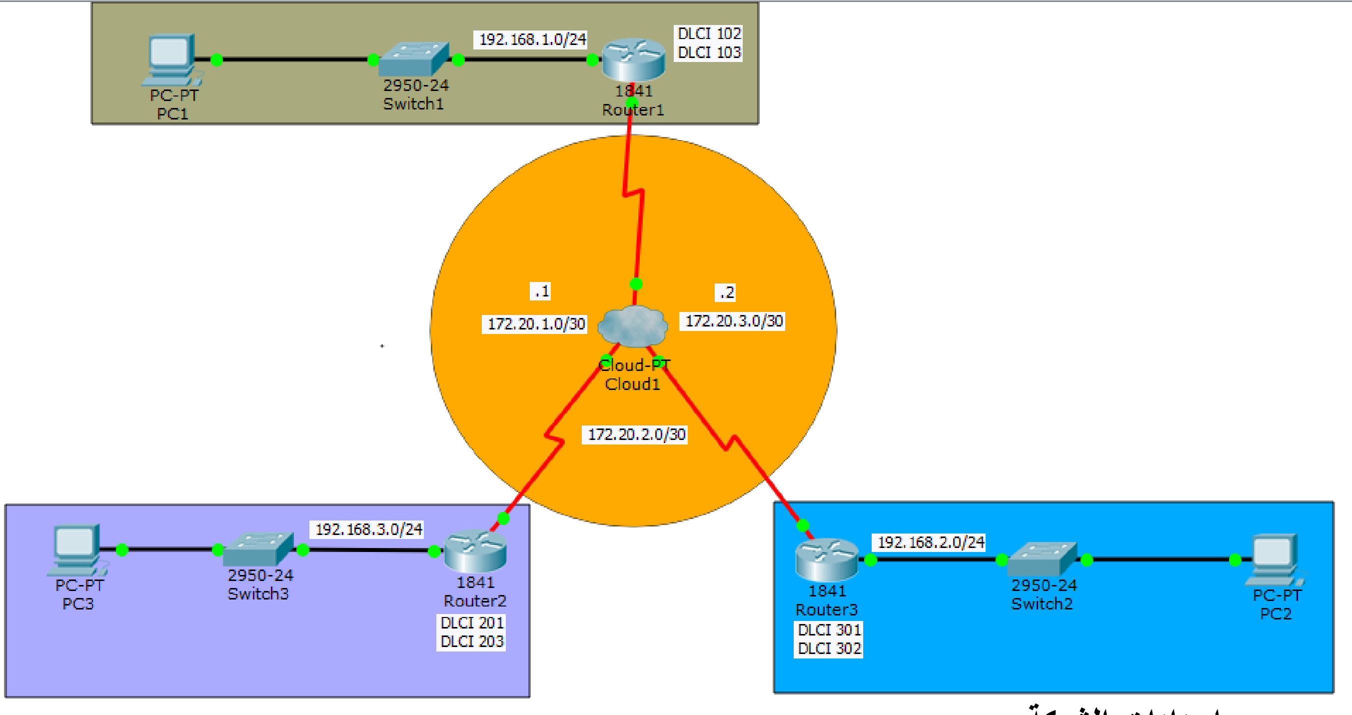
٣- الربط من خلال الفروع الرئيسية **Hub and Spoke Topology** وهذا يمثل أن يتواجد شبكة كبيرة جداً تقوم بربط جميع الفروع والشبكة ببعضهم البعض من خلال مكان واحد أو شبكة واحدة .



- الآن يكون قد تم الانتهاء من دورس تقنية الـ **Frame Relay** ونأتي لنقوم بتطبيق شبكة عملية تعمل باستخدام تقنية الـ **Frame Relay** لنكون على معرفة بعملية الاعدادات وطريقة العمل عليها ، سنقوم بعمل تطبيق مكون من ثلاث راوترات وتربط ما بينهم شبكة الـ **Frame Relay** وهي التي ستكون حلقة الربط ما بين الشبكة و الفروع ، ولكن قبل أن نبدأ في عملية التطبيق يجب أن نعلم أن شبكة الـ **Frame Relay** ليس مهندس الشبكة الموجودة في داخل الشبكة هو المسؤول عن هذه الشبكة بل شركة الاتصالات أو شركة مزودي الخدمة مهندس الشبكة فقط يكون مسؤول فقط عن الراوترات والاجهزة التي تكون في داخل الشركة فقط لا غير بينما الشبكة التي تربط ما بينا الفروع هذه من مسؤولية الشركة المستأجر منها الخط ، وهي التي ستقوم بإرسال جميع المعلومات المطلوبة التي سيقوم بها مهندس الشبكة ليقوم بربط بشبكة الـ **Frame Relay** ويتم الاتصال بالشبكة الآخر .

- الآن بعد أن تعرفنا على تقنية الـ **Frame Relay** وتعرفنا على أنواعها و طريق الربط ما بينهم و أنواع الربط سنقوم بعمل شبكة مكونة من ثلاث شبكات على مختلف المناطق، وسنقوم بربط هذه الشبكات من خلال تقنية الـ **Frame Relay** ، ولكن يجب أن نعرف بعد أن نقوم بعملية الربط من خلال الـ **Frame Relay** سيتم اتصال الشبكات المرتبطة في الـ **Frame Relay** فقط و لا نستطيع الاتصال بالشبكة الداخلية التي تتواجد مثلاً في داخل الشركة أو داخل الفرع لماذا يا ترى لأننا إذا لم نقم بتفعيل بروتوكول توجيه كيف سنعرف الشبكة الخارجية أو الشبكة الآخر ، من الطبيعي جداً أننا نحتاج لتفعيل أحد بروتوكولات التوجيه مثل الـ **OSPF** , **EIGRP** , **RIPv2** أي واحد من هذه البروتوكولات لنستطيع الاتصال بالشبكة الداخلية أيضاً .

- **سنقوم بالتطبيق على النموذج التالي كما هو موجود أسفل :**



إعدادات الشبكة :

١- سنقوم بتركيب غيمة الـ **Frame Relay** .
٢- سنقوم بتركيب ثلاث راوترات و سنتعرف الآن على إعدادات الراوترات .
٣- سنقوم بتركيب منافذ السريال على الراوترات الثلاث لنقوم بربط كوابل السريال مع شبكة الـ **Frame Relay** .
٤- سنقوم بتقسيم كل منفذ من منافذ السريال الموجودين على الراوتر إلى عدة منافذ وهمية وسنقوم بتركيب العناوين أيضاً ليستطيع الاتصال بشبكة الـ **Frame Relay**
٥- سنقوم بتفعيل بروتوكول الـ **RIPv2** على الراوتر لتستطيع الشبكات الاتصال ببعضها البعض .
٦- سنقوم بالدخول على الـ **Frame Relay** و عمل إعدادات المنافذ في داخل الـ **Frame Relay**.

- إعدادات الراوتر الأول ستكون بهذا الشكل:

(R1)

IP Address Private Network f0/0 192.168.1.1/24

IP Address Serial 0/0/0.103 172.20.3.1

IP Address Serial 0/0/0.102 172.20.1.1

Serial 0/0/0.103

Serial 0/0/0.102

DLCI 102

DLCI 103

- إعدادات الراوتر الثاني ستكون بهذا الشكل:

(R2)

IP Address Private Network f0/0 192.168.3.1/24

IP Address Serial 0/0/0.201 172.20.1.1

IP Address Serial 0/0/0.203 172.20.2.1

Serial 0/0/0.201

Serial 0/0/0.203

DLCI 201

DLCI 203

- إعدادات الراوتر الثالث ستكون بهذا الشكل:

(R3)

IP Address Private Network f0/0 192.168.2.1/24

IP Address Serial 0/0/0.301 172.20.1.1

IP Address Serial 0/0/0.302 172.20.2.1

Serial 0/0/0. 301

Serial 0/0/0. 302

DLCI 301

DLCI 302

- هذه الإعدادات الخاصة بأجهزة الراوترات الآن سنقوم بالدخول على الراوتر الأول ونقوم بعمل الإعدادات التالية:

R1

Router > **enable**

Router # **config t**

Router (config) # **hostname R1**

R1 (config) # **interface serial 0/0/0**

R1 (config-if) # **encapsulation frame-relay**

R1 (config-if) # **interface serial 0/0/0.102 point-to-point**

R1 (config-subif) # **frame-relay interface-dlci 102**

R1 (config-subif) # **ip address 172.20.1.1 255.255.255.252**

R1 (config-subif) # **interface serial 0/0/0.103 point-to-point**

R1 (config-subif) # **frame-relay interface-dlci 103**

R1 (config-subif) # **ip address 172.20.3.2 255.255.255.252**

R1 (config-subif) # **interface serial 0/0/0**

R1 (config-if) # **no shutdown**

R1 (config-if) # **exit**

R1 (config) # **interface fastethernet 0/0**

R1 (config-if) # **ip address 192.168.1.1 255.255.255.0**

R1 (config-if) # **no shutdown**

R1 (config-if) # **exit**

R1 (config) # **router rip**

R1 (config-router) # **version 2**

R1 (config-router) # **network 192.168.1.0**

R1 (config-router) # **network 172.20.1.1**

R1 (config-router) # **network 172.20.3.2**

R1 (config-router) # **end**

R1 # **copy running-config startup-config**

- الأن بعد أن قمنا بعمل إعدادات الراوتر الأول **R1** ، سنقوم بالدخول على الراوتر الثاني ونقوم بعمل نفس الإعدادات ولكن مع اختلاف بعض العناوين .

R2

Router > **enable**

Router # **config t**

Router (config) # **hostname R2**

R2 (config) # **interface serial 0/0/0**

R2 (config-if) # **encapsulation frame-relay**

R2 (config-if) # **interface serial 0/0/0.201 point-to-point**

R2 (config-subif) # **frame-relay interface-dlci 201**

R2 (config-subif) # **ip address 172.20.1.1 255.255.255.252**

R2 (config-subif) # **interface serial 0/0/0.203 point-to-point**

R2 (config-subif) # **frame-relay interface-dlci 203**

R2 (config-subif) # **ip address 172.20.2.2 255.255.255.252**

R2 (config-subif) # **interface serial 0/0/0**

R2 (config-if) # **no shutdown**

R2 (config-if) # **exit**

R2 (config) # **interface fastethernet 0/0**

R2 (config-if) # **ip address 192.168.3.1 255.255.255.0**

R2 (config-if) # **no shutdown**

R2 (config-if) # **exit**

R2 (config) # **router rip**

R2 (config-router) # **version 2**

R2 (config-router) # **network 192.168.3.0**

R2 (config-router) # **network 172.20.1.1**

R2 (config-router) # **network 172.20.2.2**

R2 (config-router) # **end**

R2 # **copy running-config startup-config**

الآن بعد أن قمنا بعمل إعدادات الراوتر الثاني **R2** ، سنقوم بالدخول على الراوتر الثالث ونقوم بعمل نفس الإعدادات ولكن مع اختلاف بعض العناوين .

R3

Router > **enable**

Router # **config t**

Router (config) # **hostname R3**

R3 (config) # **interface serial 0/0/0**

R3 (config-if) # **encapsulation frame-relay**

R3 (config-if) # **interface serial 0/0/0.301 point-to-point**

R3 (config-subif) # **frame-relay interface-dlci 301**

R3 (config-subif) # **ip address 172.20.3.1 255.255.255.252**

R3 (config-subif) # **interface serial 0/0/0.302 point-to-point**

R3 (config-subif) # **frame-relay interface-dlci 302**

R3 (config-subif) # **ip address 172.20.2.2 255.255.255.252**

R3 (config-subif) # **interface serial 0/0/0**

R3 (config-if) # **no shutdown**

R3 (config-if) # **exit**

R3 (config) # **interface fastethernet 0/0**

R3 (config-if) # **ip address 192.168.2.1 255.255.255.0**

R3 (config-if) # **no shutdown**

R3 (config-if) # **exit**

R3 (config) # **router rip**

R3 (config-router) # **version 2**

R3 (config-router) # **network 192.168.2.0**

R3 (config-router) # **network 172.20.3.1**

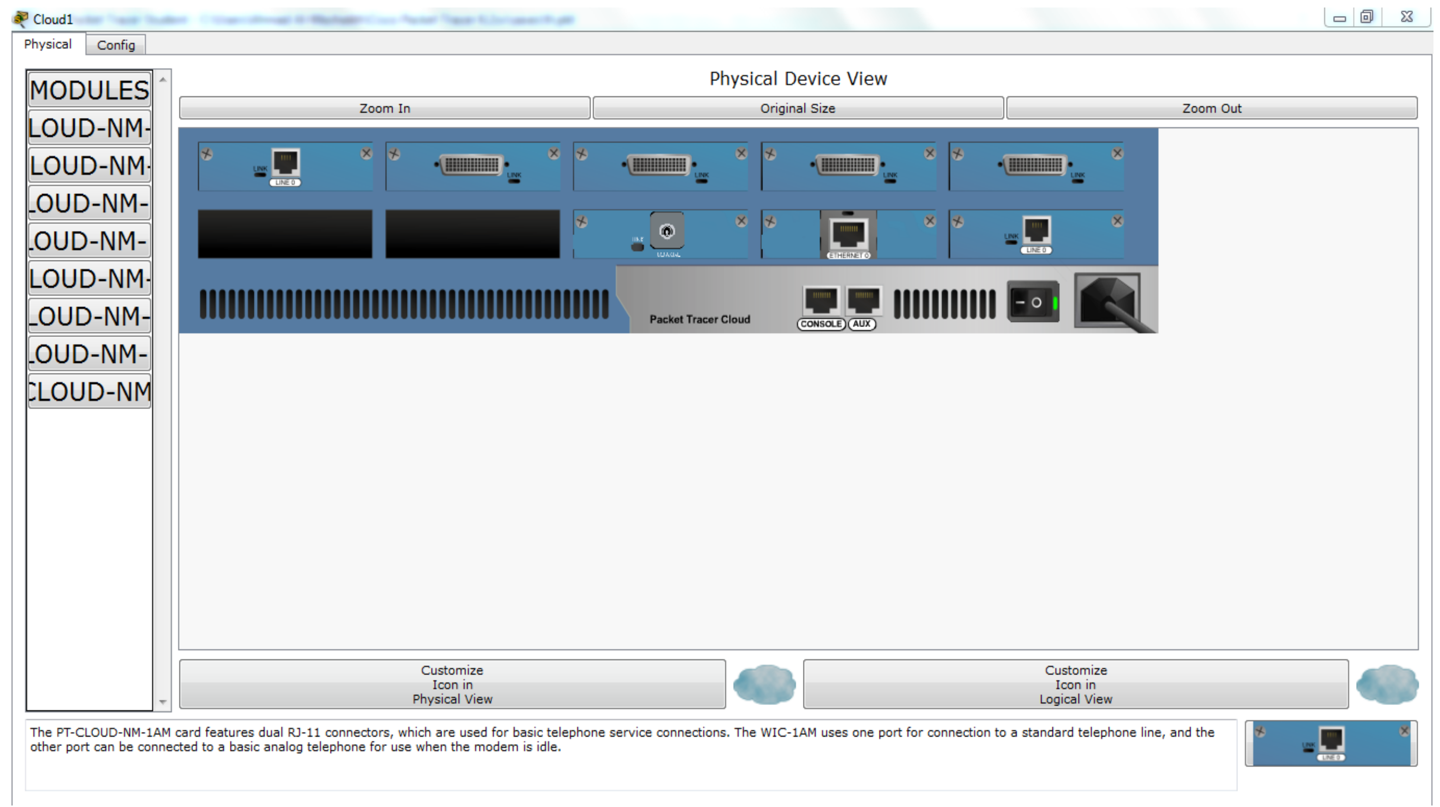
R3 (config-router) # **network 172.20.2.2**

R3 (config-router) # **end**

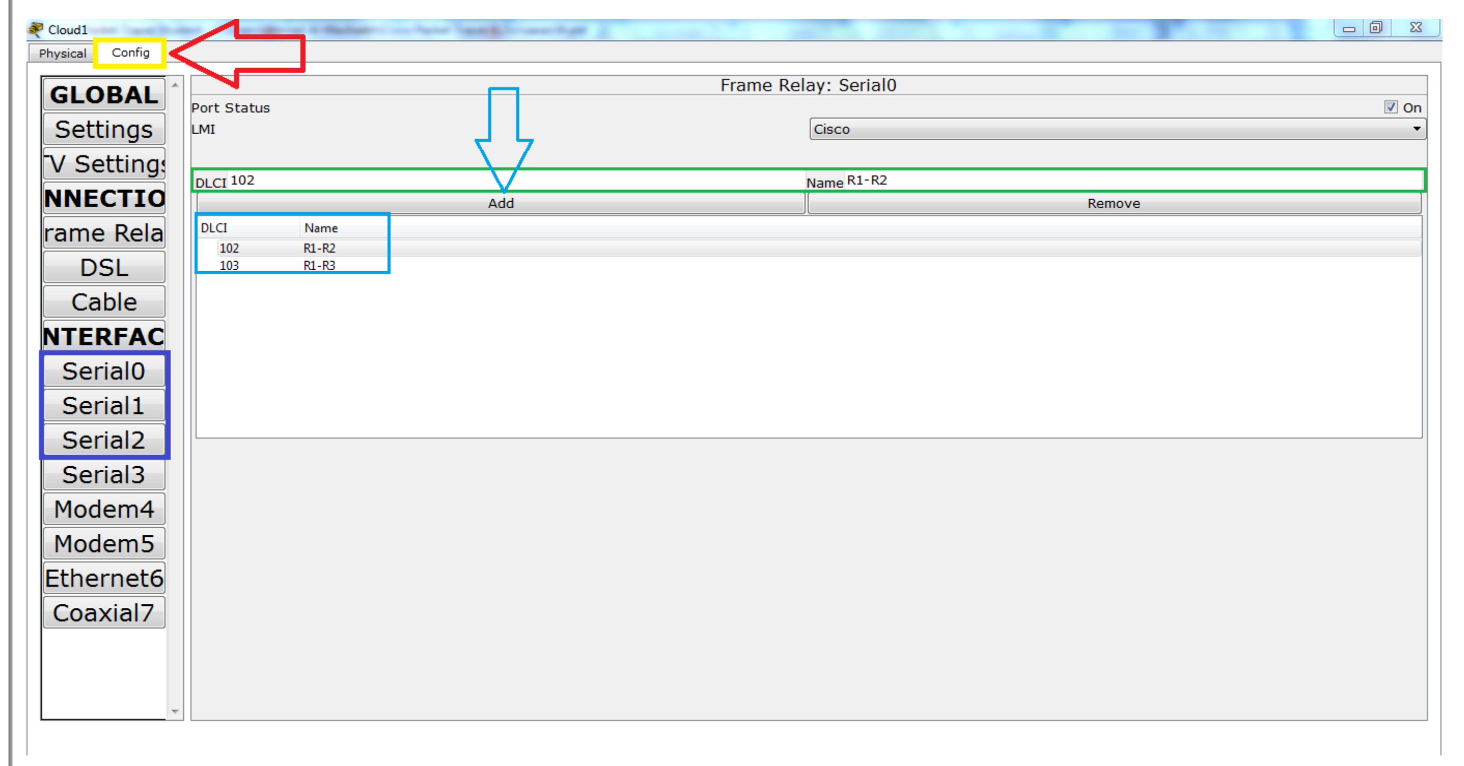
R3 # **copy running-config startup-config**

- الآن بعد أن قمنا بعمل جميع الإعدادات لجميع الراوترات سنقوم بالدخول على غيمة الـ **Frame Relay** لنقوم بعمل الإعدادات الخاصة بها لتسطيع الشبكات أن تتصل مع بعضها البعض.

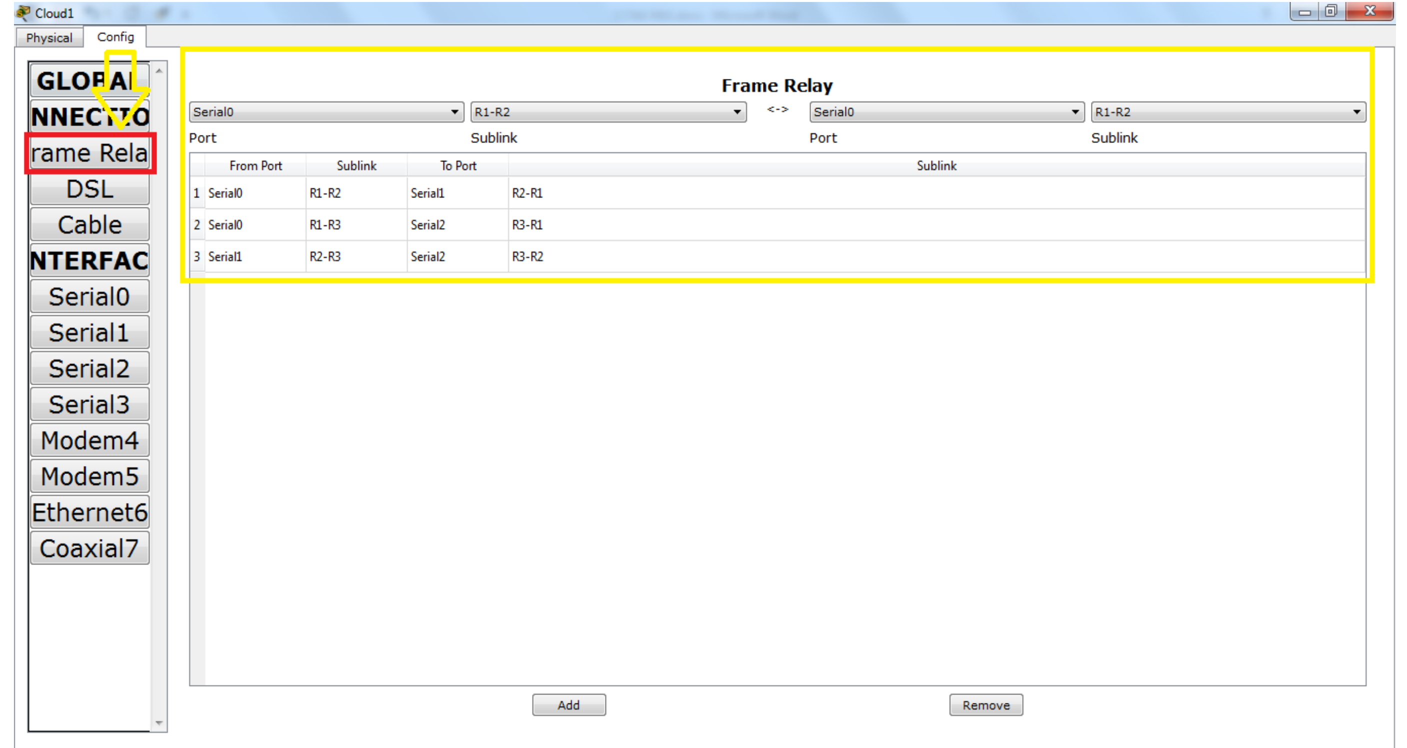
صورة الـ **Frame Relay** من الخلف انظر اليها :



- سنقوم بالدخول على خانة الـ **Config** لنقوم بعمل إعدادات منافذ الـ **Serial** كما في الصورة التالية :

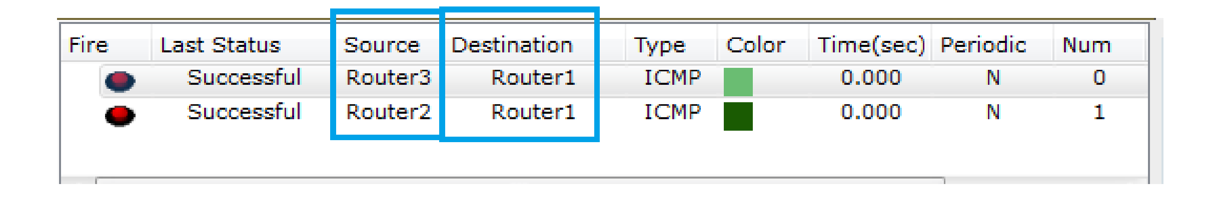


كما في الصورة سنقوم بكتابة عناوين الـ **DLCI**، لكل منفذ من منافذ السريال لتستطيع الشبكات أن تتصل مع بعضها البعض من خلال الغيمة، وبعد أن نقوم بإضافة عناوين الـ **DLCI** سنقوم بالدخول على خانة الـ **Frame Relay** الموجودة في أعلى القائمة ، كما في الصورة التالية .



- الأن بهذه الصورة سنقوم بعمل الإعدادات، سنقوم بعمل ترتيب للمنافذ فقط كما هو موضح في الصورة أعلى ونقوم بعمل إضافة ، **Add** بهذا الشكل يكون قد تم الانتهاء من إعدادات جميع الشبكات بشكل ممتاز يتقبى علينا الآن أن نقوم بعمل اختبار للشبكات لنرى هل تستطيع الاتصال ببعضها البعض أم لا ، سنقوم بعمل اختبار للرواتر المرتبطة ما بينهم الغيمة وبعدها نقوم بعمل اختبار الشبكة الفرعية الداخلية .

- سنقوم بعملية الاختبار عن طريق إرسال **Packets** لجميع الراوترات المتصلة من خلال الغيمة، في حال تم كتابة **Successful** هذا يعني أن الراوترات تستطيع الاتصال ببعضها البعض ، ولكن إذا تم كتابة **Faill** هذا يعني على أنه لا يوجد اتصال ما بين الشبكات و يوجد مشكلة في الإعدادات .



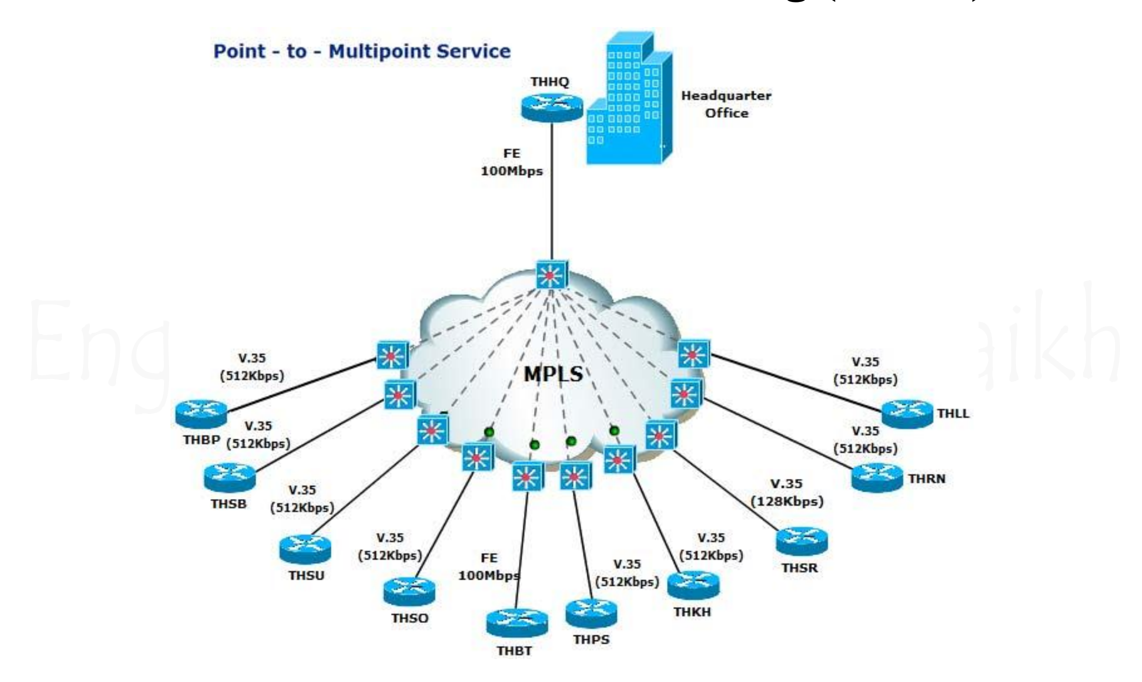
Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num
	Successful	Router3	Router1	ICMP		0.000	N	0
	Successful	Router2	Router1	ICMP		0.000	N	1

- نلاحظ أنه تم رد النجاح برسالة الـ **Successful** هذا يعني أن جميع الراوترات تستطيع الاتصال مع بعضها البعض يتبقى علينا اختبار الشبكات الفرعية الموجودة في داخل الفروع كما نلاحظ في الصورة التالية :

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num
	Successful	PC2	PC1	ICMP		0.000	N	0
	Successful	PC2	PC3	ICMP		0.000	N	1

كما نلاحظ أنه تم الاتصال بشكل صحيح و هذا يدل على أن جميع الشبكات متصلة مع بعضها البعض .

Multi Protocol Label Switching (MPLS)



MPLS: هو عبارة عن تقنية لنقل البيانات وتعمل هذه التقنية مع الشبكات الواسعة **WAN**، حيث تقوم هذه التقنية بوظيفة ربط الشبكات المحلية ببعضها البعض عن طريق الشبكة الواسعة ولكن الاعتماد يكون على الـ **MPLS** مثل تقنية الـ **Frame Relay** ولكن في تقنية الـ **MPLS** يتم نقل البيانات بشكل أسرع وحجم البيانات يكون أصغر ، ويجب أن نعلم أن هذه التقنية تعمل مع الطبقة الثانية من طبقة الـ **OSI Layers** و هذا يدل على أنها لا تحتاج لعنوان الـ **IP** فهذه الطبقة لا تعمل مع الطبقة الثالثة التي تعمل مع العناوين الـ **IP** والتي تكون على شكل **Packets** ، بينما في الطبقة الثانية تعمل البيانات على شكل إطار **Frame** ويعتمد هذا الإطار على العنوان الفيزيائي الماك ادرس.

تقنية الـ **MPLS** معتمد عليها أو يتم العمل عليها بشكل كبير في شركة مزودي الخدمة مثل شركة الانترنت وشركة الاتصالات التي تقوم بربط وتوصيل الشبكات ببعضها البعض لهذا السبب تكون في أغلب الاحيان لن تجد أحد يعمل بهذه التقنية إلا شركة الاتصالات.

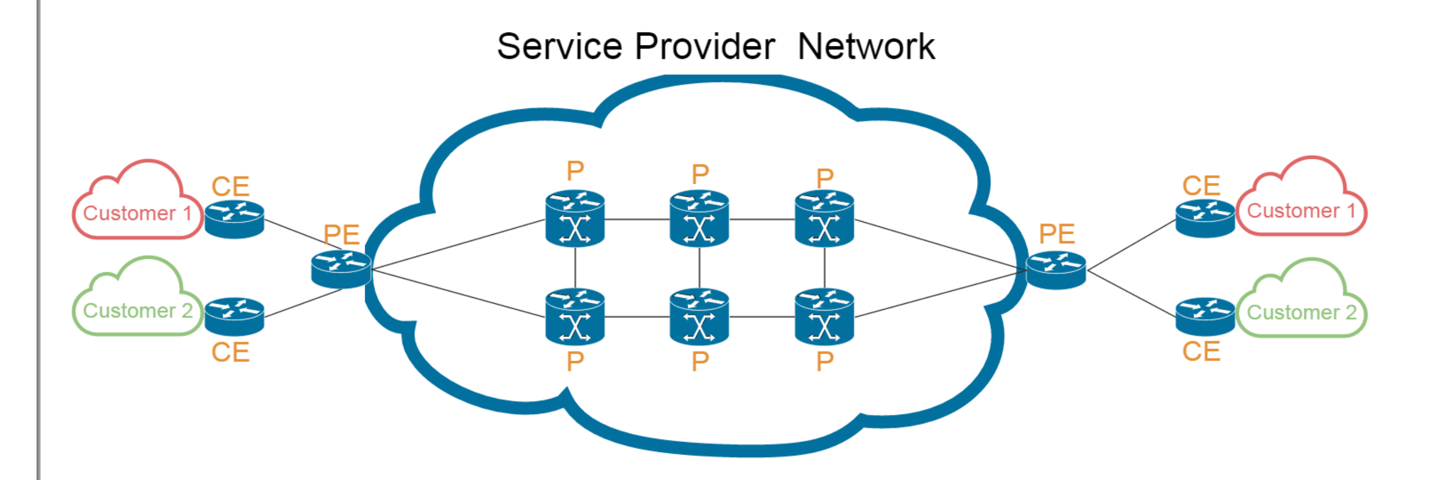
مقسم البروتوكولات المتعددة في تقنية الـ **MPLS** هي التكنولوجيا الجديدة التي تقدم لفتح شبكة الإنترنت من خلال توفير العديد من الميزات الإضافية وخدمات التطبيقات التي تستخدم بروتوكولات الانترنت مثل **Frame Relay, ATM, or Ethernet**. تقسم البروتوكولات المتعددة باستخدام تسميات البيانات إلى تقسيم حزم البيانات. يجب أن يتم توزيع هذه الحزم بين العقد التي تشكل الشبكة. العديد من الخدمات الجديدة التي تريد مزودي خدمة الإنترنت لتقديم وظائف تعتمد على هندسة المرور. هناك حالياً توزيع تسمية اثنين من البروتوكولات التي توفر الدعم للهندسة المرور ، بروتوكول حجز الموارد (**RVSP**) والقيد على أساس التوزيع تسمية دأب البروتوكول (**CR-LDP**). على الرغم من أن هذين البروتوكولين يعملان على تقديم مستوى مماثل من الخدمة، إلا أن الطريقة التي يعملون بها مختلفة، تعمل البروتوكولات على تقديم معلومات واضحة وذلك عند الحاجة للمساعدة على تحديد أي بروتوكول لتنفيذه في حركة المرور هندسة شبكة مقسم البروتوكولات المتعددة. كل بروتوكول وحامل اللقب. مع التسليم بأن اختيار بروتوكول توزيع التسمية هو أمر حاسم لنجاح الجهاز وهذه المقالة تفسر التشابه والاختلافات بين هذين البروتوكولين، للمساعدة في تحديد البروتوكول الذي هو واحد الحق في استخدام في خاصة بالبيئة. مقسم البروتوكولات المتعددة تقدم حلولا لكل **RSVP** و (**CR-LDP**) بالإضافة أنها أحد تقنيات التي تعتمدها شركة **Cisco** في أجهزة الحديثة، وهذه روابط الشركة التي قد تلقى فيها معلومات عديدة عن هذه التقنية .

- **أجهزة تقنية الـ MPLS :**

١- **Provider Router (P):** هذا الجهاز يتواجد في شركات مزودي الخدمة **ISP**.

٢- **Provider Edge (PE):** هذا الجهاز الذي يقوم بعملية الربط ما بين أجهزة المستخدمين و أجهزة مزودي الخدمة مثل الراوترات والسويتشات.

٣- **Customer Edg (CE):** هذا الجهاز هو الخاص في المستخدمين وهو الجهاز الذي يقوم بربط الشبكات المحلية **LAN** في الشبكة الواسعة **WAN**.



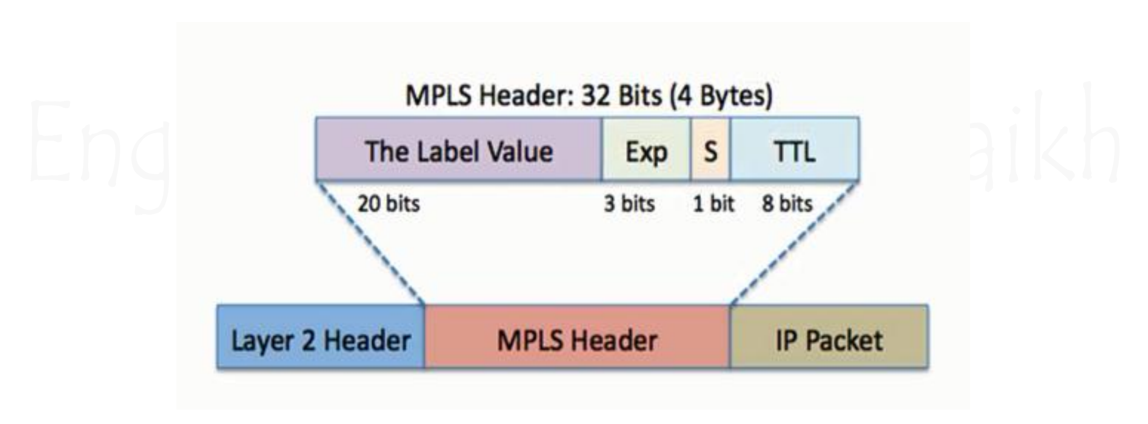
تنقية الـ MPLS تعمل وتعتمد على الـ Label :

تقنية الـ **MPLS** تعمل وتعتمد على الـ **Label** الملاصق في عملية إرسال البيانات بدلاً من أن يتم إرسال الـ **Header** الذي كان يرسل في كل رسالة من البيانات حيث كان يقوم بجمع مجموعة من البيانات مثل عنوان المرسل وعنوان المستقبل ونوع البيانات المرسلة والكثير من المعلومات التي قمنا بذكرها في الدروس السابقة، ولكن عندما ا يتم الاعتماد على تقنية الـ **MPLS** في عملية إرسال البيانات ستتم عن طريق الـ **Label** والتي تتواجد في داخل تقنية الـ **MPLS** حيث أنها لا تعتمد على العناوين أو جدول العناوين مثل الـ **Routing Table** الذي يتم تجميعها في داخل الراوترات ، حيث أنه يجعل الاعتماد كله على الـ **MPLS Label** حيث تكون أسرع بكثير في عملية الإرسال والاستقبال ويتم فقط وضع الـ **Label** في الباكيت المرسلة .

لنتعرف أكثر على طريق تكوين الـ **Label** يتم تركيب الـ **Label** ما بين الخانات التالية:

Layer 2 Header [MPLS Header] IP Packets

وسيكون حجم الـ **MPLS Header** **32 bits** وسيكون ثابت ولن يتغير أبداً وسيكون أيضاً مقسم إلى أربعة اقسام كما في النموذج التالي :



- معلومات مهمة جداً يجب أن نكون على معرفة بها :

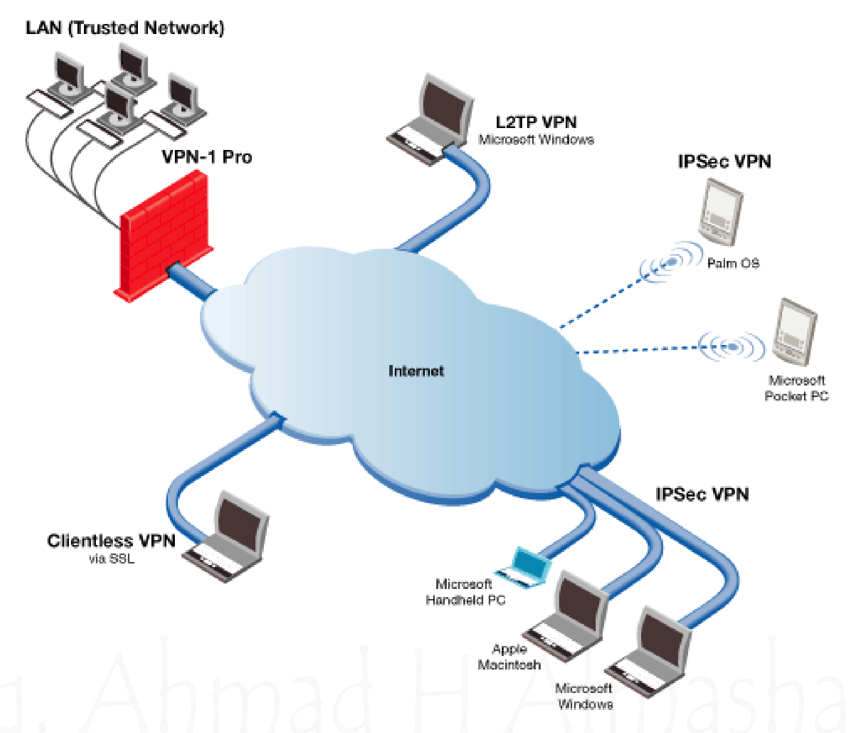
١- يجب أن نعلم أن البيانات التي يتم إرسالها واستقبالها ستمر من خلال مزودي خدمة الانترنت **ISP** ، أو من خلال شركة الاتصالات بهذه المعلومات يجب أن نعلم أن في عملية الإرسال أو الاستقبال يستطيع مزودي الخدمة، أو شركة الاتصالات أن يعرفو مسار البيانات المرسلة لأنه تمر من داخل الشبكة الخاصة بهم،الآن ما الذي يستطيعون أن يعرفوه ، يستطيعون معرفة العناوين لأنه شركة مزودي الخدمة تعمل على تحديد المسارات فيستطيع معرفة العنوان الخاص بك وإلى أين ذاهب ،ولكن لا يستطيع أن يعرف البيانات المرسلة .

٢- هذا لا يعني أن المرسل والمستقبل في أمان لا بل يستطيع مزودي الخدمة أن يقرؤوا البيانات المرسلة، والمستقبل فقط يقوم بتحويل مسار الباكيت للهدف المطلوب لديه على أحد الشبكات و يقوم بعرض كل حرف مرسل في الباكيت ولكن من الطبيعي جداً أن هذا الشيء غير مصرح له في شركة مزودي الخدمة ،أو شركة الاتصالات ولا ننسى أنها مسؤولية على الشركة العملاقة في هذه المواضيع .

VPN

Virtual Private Network

الشبكة الخاصة الافتراضية

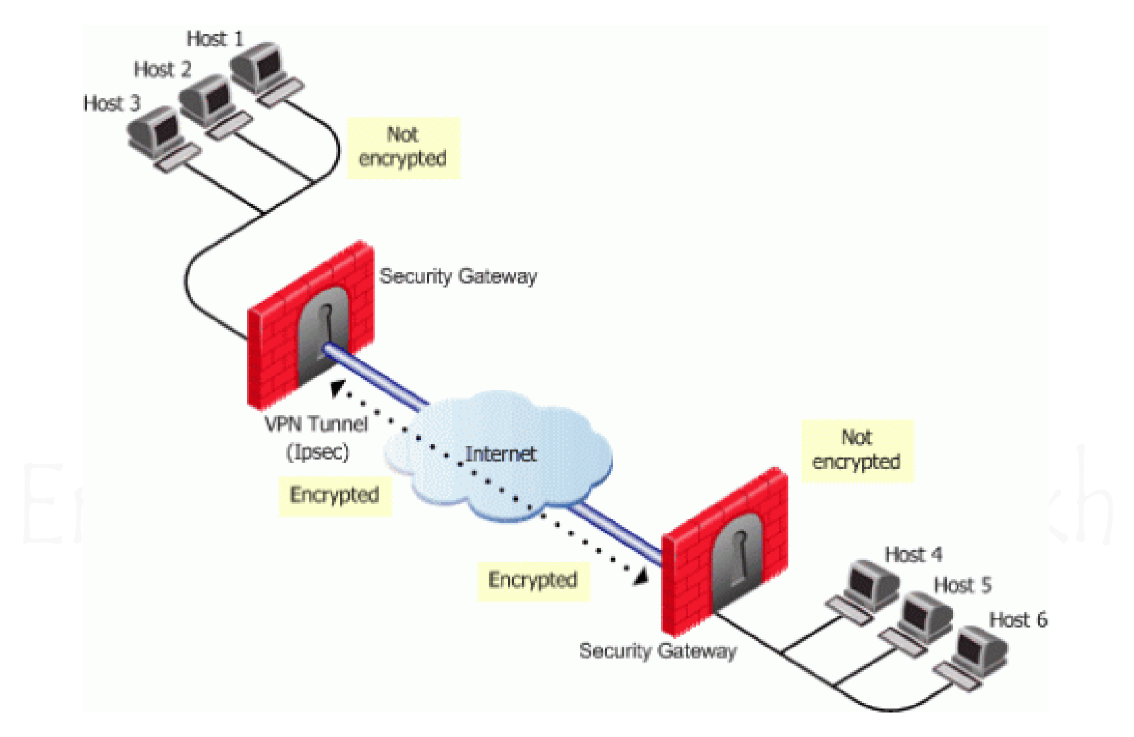


VPN : هي عبارة عن خدمة مهمة جداً وتستخدم بشكل كبير جداً، ولها عدة أنواع سنقوم بذكرهم لاحقاً ولكن يجب أن نعرف ما هي وظيفة هذه الشبكة الافتراضية الوهمية وظيفتها الأساسية هي الاتصال عن بعد أو الوصول عن بعد **Remote Access** ، مثلاً لدينا شركة وهذه الشركة يوجد فيه السيرفرات أو الخوادم ولكن طالما متواجدين في داخل الشركة لن نحتاج للدخول عن طريق خدمة الـ **VPN** ولكن نحتاج خدمة الـ **VPN** عندما يريد أحد الموظفين الدخول على السيرفرات من المنزل أو من الخارج بعد خروجها من الشركة من الطبيعي جداً سنقوم بعمل إعدادات سيرفر لخدمة الـ **VPN** لتقوم بعمل وإدارة هذه التقنية ويجب أن نعلم أيضاً أن هذه التقنية تحتاج لشركة الانترنت لنستطيع الاتصال بخوادم الشركة والعمل بشكل صحيح ، سنقوم بشرح مميزات هذه التقنية والانواع كل نوع لديه مميزاته ولديه عيوبه سنتعرف على كل من هذه الانواع بالتفصيل ، لنستطيع المعرفة الجيدة لهذه التقنية في حالة نريد بناء هذه الشبكة الوهمية الافتراضية يجب أن نكون على دراية كاملة أي نوع من أنواع الـ **VPN** سيتم استخدامه والعمل عليه .

VPN: هي الشبكة الافتراضية وهي نفسها الشبكة العنكبوتية، ولكن تم توظيف خصائصها لتكون سرية في عملية نقل البيانات والحفاظ على سرية المعلومات وأمان لأن البيانات تنتقل في شبكة الانترنت ولا ننسى أن شبكة الانترنت مفتوحه على جميع أنحاء العالم وهذا يشكل خطر كبير على البيانات التي يتم إرسالها واستقبالها لهذا السبب تم اختراع خدمة الـ **VPN**، تكون البيانات في أمان لأنها تقوم بعمل قناة مشفرة لنقل البيانات المرسلة.

- **لنتعرف على كيفية حماية البيانات في شبكة الـ VPN الافتراضية :**

تبدأ حماية البيانات بشكل عام بعملية التشفير بحيث يصعب فهمها إذا تم سرقتها، و لكن حتى لو تم تشفير المعلومات لا يكفي ولا نعتقد أنه لن يتم كسر أو تحليل هذا التشفير ،أحيانا إذا وضعنا بعين الاعتبار وجود أنواع كثيرة من آليات التشفير والتي يمكن كسرها بطريقة أو بأخرى وما أكثر الأمثلة هنا بدأت بسرقة أرقام البطاقات الائتمانية انتهت بسرقة البرامج القيد البرمجة من أصحابها وغيرها الكثير من الأمثلة، لذلك كان لابد دائما من اتباع لوغارتمات قوية ومؤكدة من شركات كبيرة وذات اسم لامع في عالم التشفير كنقطة مبدئية للعمل على هذه الشبكات الافتراضية .



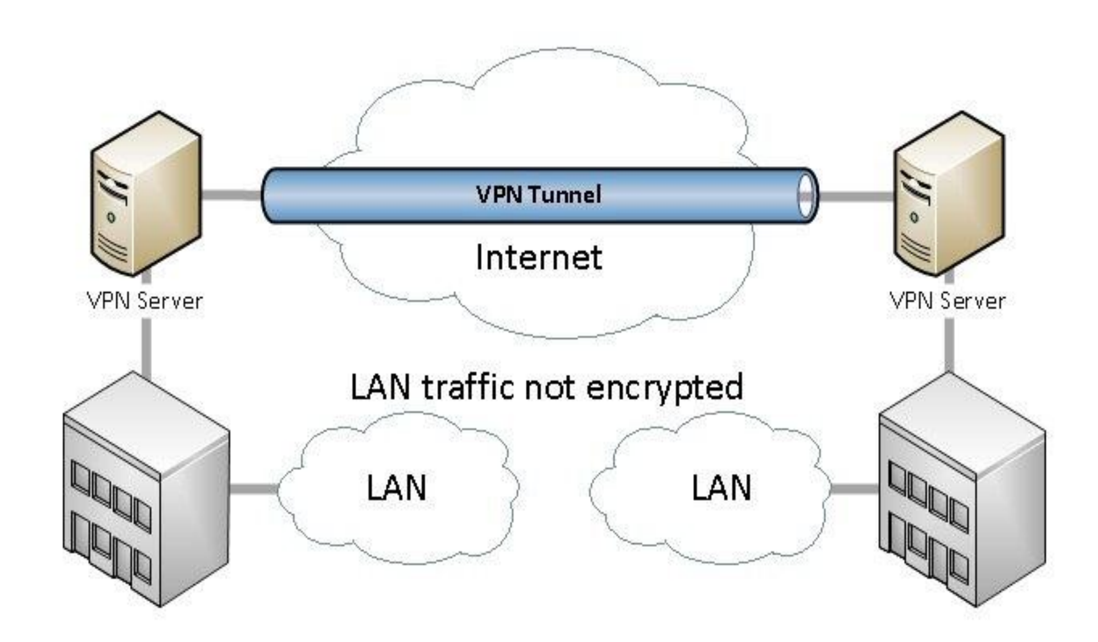
- **لنتعرف على مكونات الشبكة الافتراضية التي تعمل على تكملة إعدادات هذه الشبكة :**

المكونات التي تعتمد عليه الشبكة الافتراضية هي المكونات الاساسية المهم جداً ولا يمكن الاستغناء عنها ابداً ، الشبكة تتكون من مضيف أو المستخدم و الخادم أو السيرفير حيث يتم عمل الإعدادات الخاصة بشبكة الـ **VPN** على الخوادم أو السيرفرات وربطهم على شبكة الانترنت ليستطيع المستخدم الذي يكون خارج نطاق الشركة مثل في البيت أو في مكان ما ، ليستطيع الاتصال في السيرفرات والدخول على الشبكة والعمل بشكل طبيعي ولكن هذا أيضاً يدل على أنه سيتم عمل إعدادات للمستخدم ليستطيع الاتصال بشبكة الشبكة الداخلية من الطبيعي جداً سيتم عمل سيرفر **VPN** ونقوم بإنشاء مستخدمين في داخل هذا السيرفر وبعدها سنقوم بتوزيع أسماء المستخدمين للموظفين المصرح لهم بالدخول عبر شبكة الـ **VPN** .

- الآن بعد أن تعرفنا على الشبكة يجب أن نعلم أننا سنحتاج اتصال بشبكة الانترنت هذا يعني أنه سيتم استخدام عنوان عام **IP Public** الذي يكون على الانترنت لنستطيع الاتصال في الشبكة الخاص في الشركة ، من البيت أو من مكان آخر.

يتم إرسال البيانات في الشبكة الافتراضية الـ **VPN** بشكل منسق و آمن أكثر بكثير من أي عملية إرسال أخرى مثل ، يتم إرسال البيانات عبر بوابة الاتصال **GateWay** ويتم أيضاً تحديد الشبكة المرسل إليها البيانات **Target Network** ويكون أيضاً معرف بجميع المعلومات ما قبل عملية الاتصال والإرسال ويكون أيضاً تم معرفة المستخدم **Clients** الذي سيقوم بعملية الاتصال و عملية الإرسال .

الشبكة الخاصة الافتراضية هي عبارة عن توصيل أو ربط جهازين أو شبكتين ببعضهم البعض عن طريق شبكة الإنترنت كما هو موضح في الصورة التالية أسفل و هي تقنية تعتمد في عملها على بروتوكول حيث يطلق على عملية إنشاء الاتصال الخاص ما بين جهازي حاسوب من خلال شبكة وسيطة كالإنترنت اسم ناقل البيانات عبر مسار آمن(**Tunneling**) حيث يتم إنشاء هذا المسار بين جهازي حاسوب بشكل مباشرة .



- **VPN Tunneling:** هو عبارة عن معلومات خاصة ومشفرة يتم تبادلها ما بين الجهازين المتصلين ببعضهما البعض عن طريق شبكة الـ **VPN** و عند استلام المعلومات للجهاز المطلوب سيتم فك التشفير عن المعلومات و عرضها للمستخدم.

- ويوجد بروتوكولان لعملية نقل البيانات بشكل آمن و هما مختصان في نظام الحماية:

Point – T – Point Tunneling Protocol (PPTP)

Layer Two Tunneling Protocol (L2TP)

- هذه البروتوكولات المختصة في تأمين و تشفير البيانات في عملية النقل.

Secure Socket Tunneling Protocol (SSTP)

VPN, Security Protocol (IPSec)

- **التطبيقات الأمينة لخدمة الـ VPN يتم الاعتماد عليها في عملية تنقل البيانات في داخل قناة النقل الخاصة في شبكة الـ VPN ، وتنقسم إلى أربعة مهام .**

١- المصداقية **Authentication** ما بين المتصيلين، ويجب أن تكون المصداقية عالية جداً ما بين المرسل و المستقبل .

٢- الحفاظ على سلامة البيانات **Data Integrity** أثناء عملية نقل البيانات سيتم المحافظة على سلامة البيانات بشكل كامل حتى يتم وصولها للجهاز المطلوب وفك التشفير عنها .

٣- خصوصية البيانات **Confidentiality** تكون البيانات مغلفة بشكل كامل ، حيث لا يستطيع أي أحد أن يفهم هذه البيانات إلى المستخدم المطلوب فقط هذه الخصوصية تكون من معلومات المستخدم المستقبل .

٤- مضاد إعادة الإرسال **Anti – Reply** يتم استخدام هذه الخاصية في حالة تم اصطياد البيانات من أحد المخترقين ، في هذه الحالة لن يتم إرسال البيانات مرة أخرى إلا بعد أن يقوم المستخدم من التأكد من أنه القناة محمية بشكل كامل .

فوائد تطبيق شبكة الـ VPN :

١- تقليل التكلفة **Cost Saving** عندما ا نستخدم تقنية الـ **VPN** فانها لا تكلف كثيراً مثل خطوط الاتصالات التي تشترك فيه بشكل رسمي، على عكس تقنية الـ **VPN** قليلة التكلفة و تحتاج فقط عنوان عام **IP Public** .

٢- الوصول عن بعد **Remotely Connection** الاتصال عن بعد مثلاً نريد الاتصال من البيت بالشركة عن بعد من خلال شبكة الانترنت ولكن بطريقة خاصة عن طريق شبكة الـ **VPN** .

٣- نستطيع توسيع الشبكة كما نريد **Scalability** ،مثلاً عندما ا نريد تكبير حدود الشبكة ونريد أن نقوم بإضافة مستخدمين أكثر من السابق .

٤- أكثر أمان وحماية للبيانات **Security** تكون البيانات في سرية و حماية و أمان أفضل بكثير من أن تسير البيانات في خطوط شركة الاتصالات ومزودي الخدمة ، ولكن في شبكة الـ **VPN** تسير البيانات في قناة خاصة ما بين المستخدم والطرف الآخر بشكل مباشر ومن غير تدخل وسيط ينقل البيانات ما بينكم .

أنواع شبكة الـ VPN :

في شبكة أو تقنية الـ **VPN** يوجد عدة أنواع ، بينما كل الانواع تعمل بنفس الفكرة ولكن مع اختلاف طريقة الإعدادات والمميزات بين كل نوع ، سنقوم بذكر هذه الأنواع وشرحها :

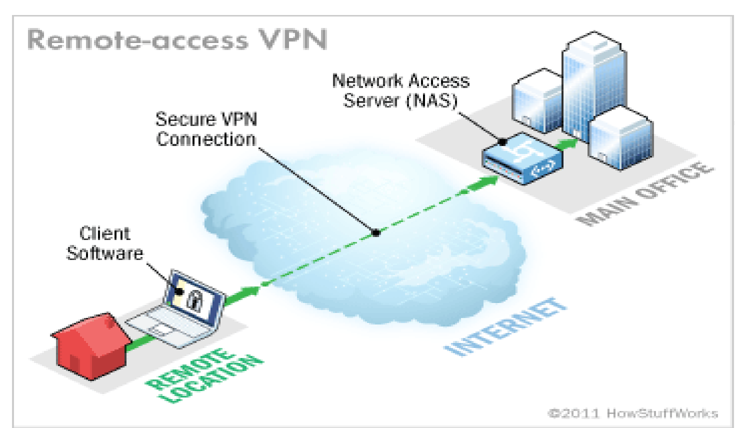
أنواع الـ VPN :

1- Dial – up VPN
2- Point to point VPN (IP VPN)
3- Site to Site VPN
4- Site to Multi Site VPN (DM VPN)
5- MPLS VPN

١. Dial – up VPN

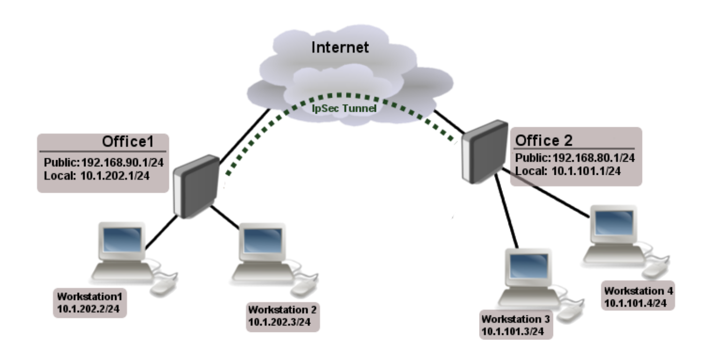
هذا النوع من شبكة الـ **VPN** مستخدم في الشبكات التي يتم الاتصال فيها عن بعد، مثلاً عندما ا نريد الاتصال بالشركة نحن موجودين في المنزل ونريد الدخول على شبكة الشركة سنقوم بعمل إعدادات الـ **Dial – up VPN** ونقوم بتزويد المستخدم بمعلومات الشبكة الداخلية ليستطيع الدخول على شبكة الشركة .





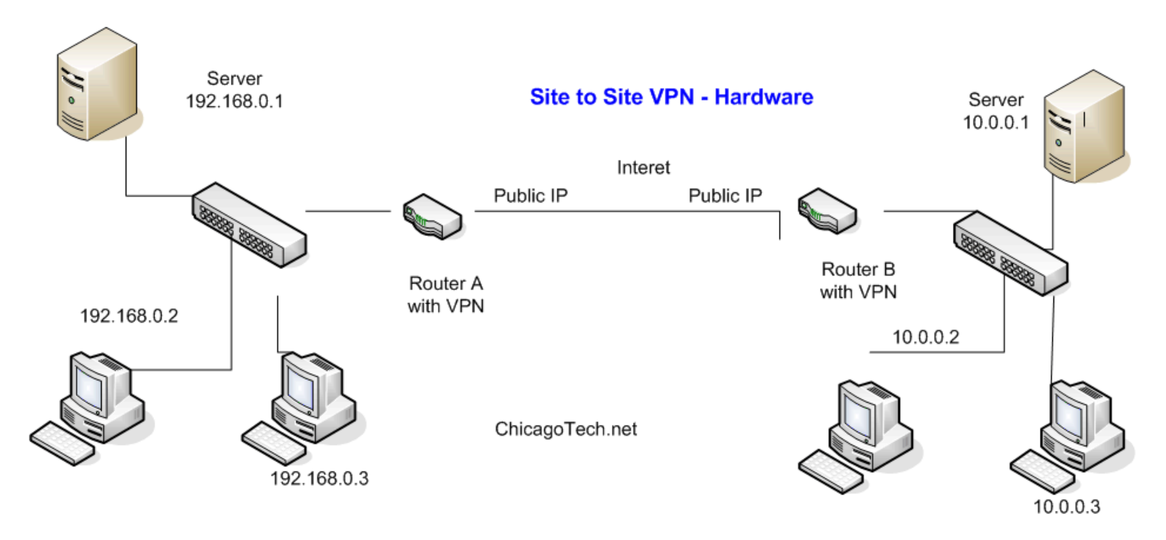
٢. Point to point VPN (IP VPN)

هذه النوع من شبكة الـ **VPN** تقوم بعمل اتصال ما بين شبكتين من نوع الـ **VPN** ولكن عن طريق شركة الاتصالات أو مزودي الخدمة لنستطيع ايصال الشبكات مع بعضها البعض وكأنهم في شبكة واحدة.



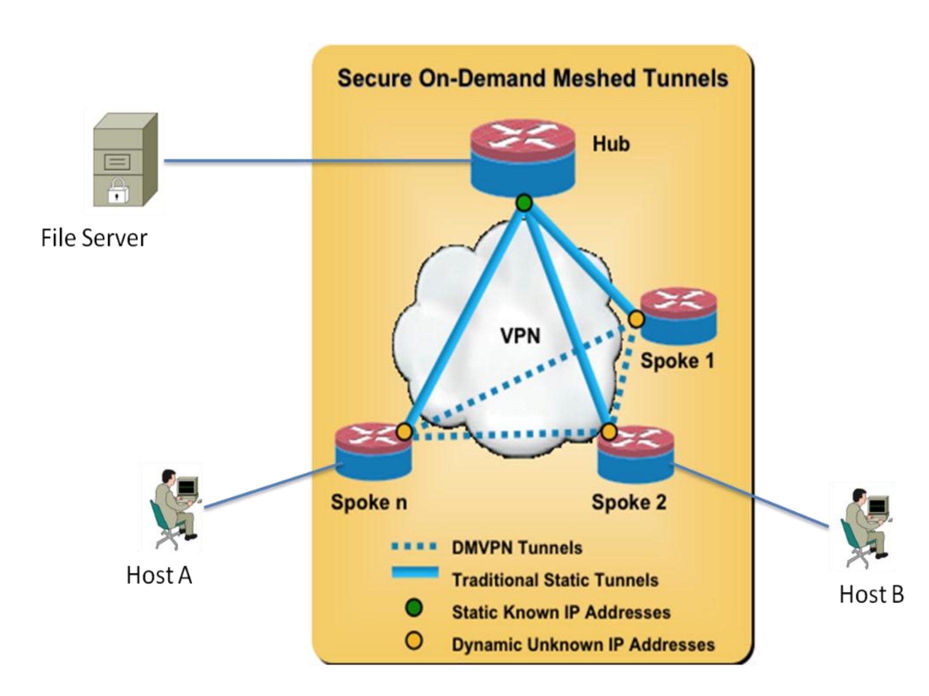
٣. Site to Site VPN

هذا النوع يقوم بربط شبكتين ببعضهم البعض ، مثلاً عندما ا يكون للشركة أكثر من فرع ونريد أن نربط الفروع لتستطيع أفرع الشبكات الاتصال مع بعضهم البعض وتعمل وكأنها في شبكة واحدة ، ويجب أن نعلم أيضاً أننا نستطيع الربط من أكثر مزود خدمة على مختلف الشركات بشكل طبيعي جداً على عكس الـ **Point to point VPN** الذي يحتاج أن يكون الاتصال من شركة مزودي الخدمة نفسها .



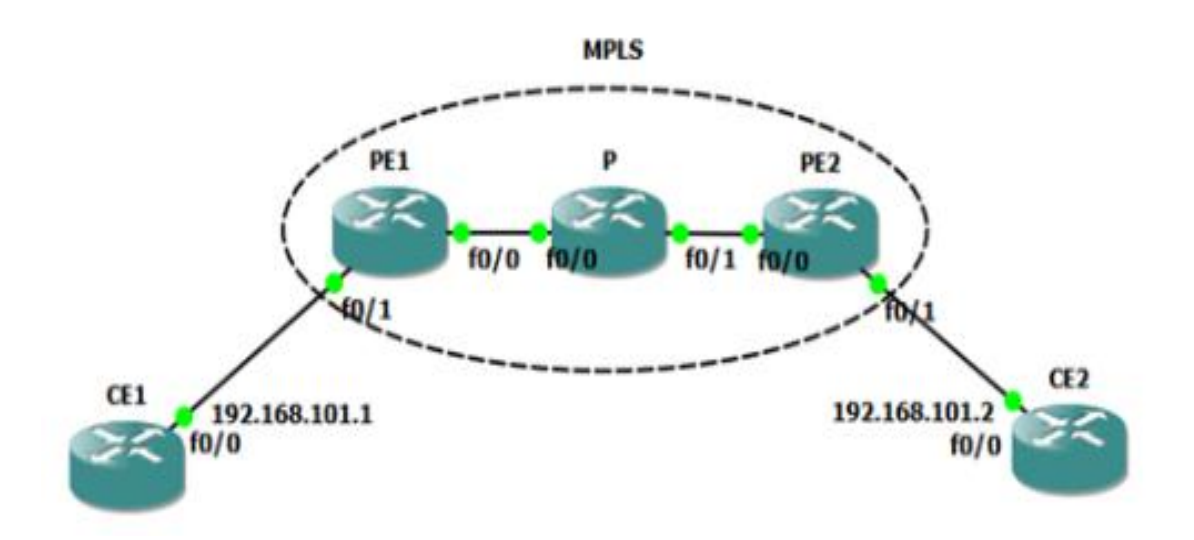
٤. Site to Multi Site VPN (DM VPN)

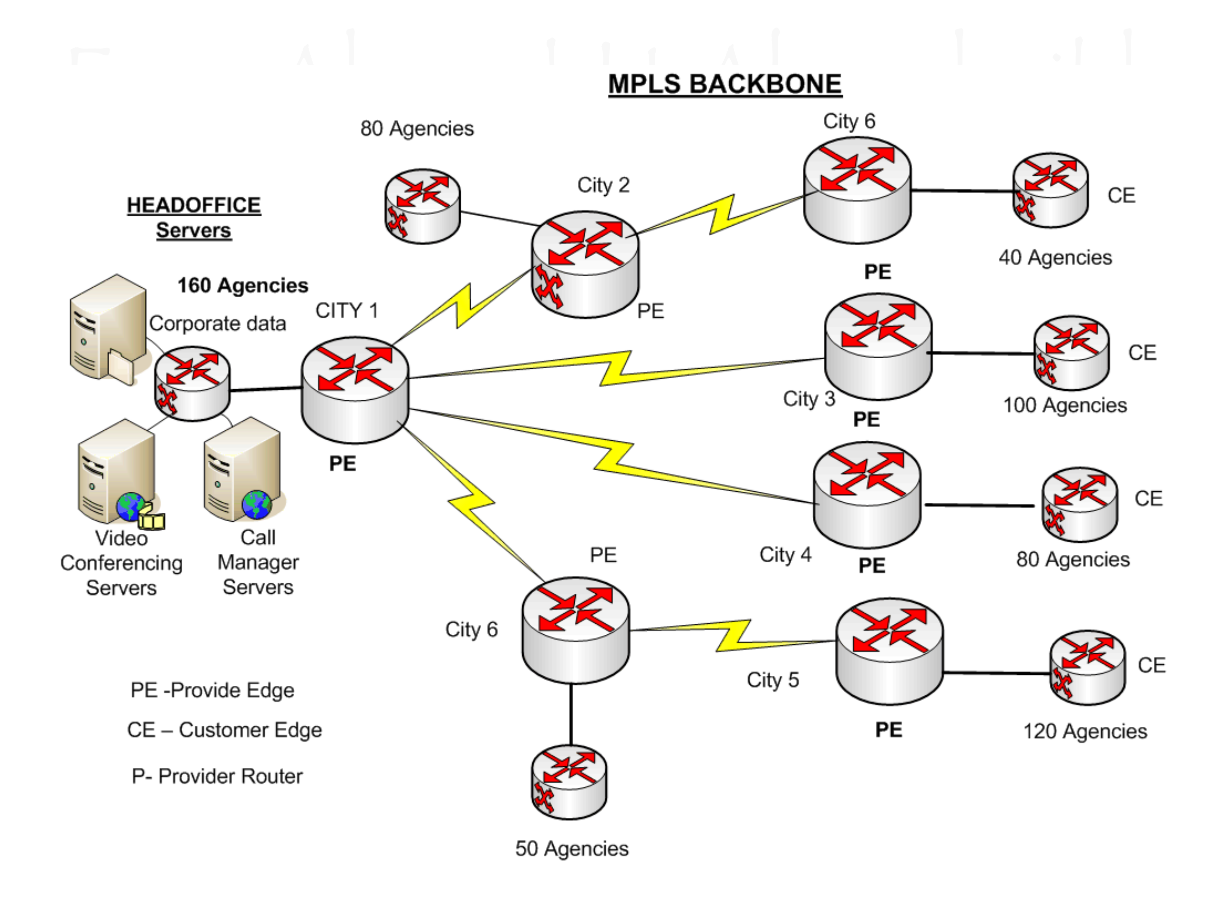
هذه الشبكة تعمل بشكل مختلف عن الشبكات التي قمنا بذكرها من قبل ، و من مميزات هذه الشبكة أنها تحتاج أن يكون فرع رئيسي في أحد فروع الشركة ليتم الاتصال ما بين الفروع الآخرى.



٥. MPLS VPN

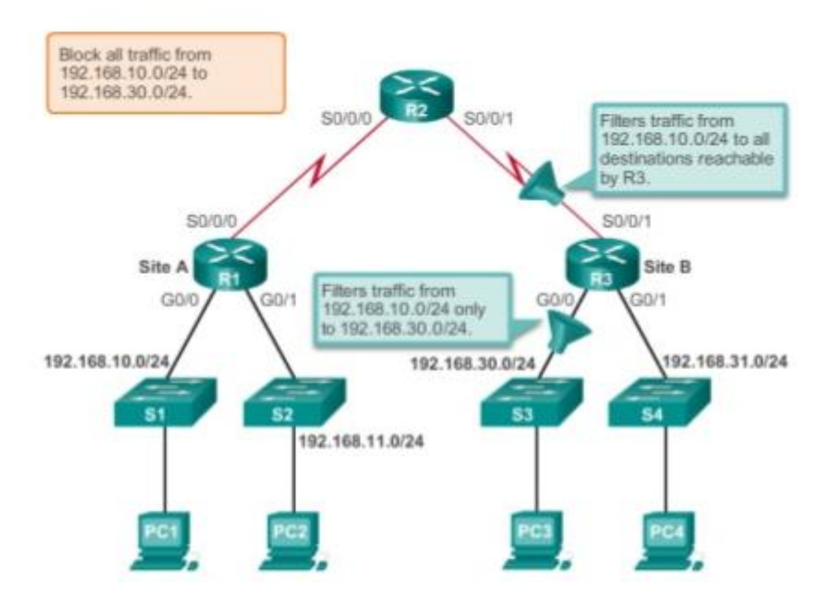
هذه الشبكة تعمل مع تقنية الـ **MPLS** والتي تعمل بشكل شبكة **VPN** وتم العمل عليها بشكل جديد وليس قديم .





فهرس المستوى الخامس أمن وحماية الشبكات

Access Control Lists (ACL)



ACL : هي تقنية تقوم بالتحكم في عملية الاتصال ما بين الشبكات وتقوم بتحديد الأجهزة أو الشبكات المصرح لها بالدخول ، والشبكات الغير مصرح لها بالدخول وذلك يتم من خلال تسجيل عناوين الشبكات أو عناوين الأجهزة في قائمة المنع أو قائمة الوصول ، حيث أنه بهذا الشكل تكون الشبكة أكثر أمان و تنسيق أكثر عندما ا نقوم بعملية المنع وعملية السماح .

- **فوائد و مميزات الـ ACL :**

١- تستخدم في الشبكات الكبيرة والصغيرة وتوفر لنا عملية التصفية للبيانات الغير مصرح لها بالدخول لشبكة أخرى.

٢- حماية الشبكة من الوصول مثل منع موظفين في شبكة معينة الوصول لشبكة الانترنت أو الوصول لشبكة السنتر أو الاتصال بأحد سيرفرات الويب .

٣- تستطيع شبكة الـ **ACL** عمل الـ **Filtering** للبيانات لتقوم بمعرفة هذه البيانات إلى أين ستصل و هل مصرح لها بالدخول أم لا .

٤- تعمل هذه التقنية في طبقة الـ **OSI Layer** تبدأ من الطبقة الثالثة والرابعة.

٥- يجب أن نعلم أن هذه الشبكة لن تقوم بمنع الفيروسات في الشبكة مثل الانتي فيروس لأنها ليست من وظيفة الـ **ACL**.

٦- يجب أن نعلم أيضاً أنه لا تكفي عن الفايرول الذي يمنع عملية الاختراق والتجسس.

٧- تعمل على جهاز الراوتر وخاصة على المنفذ تعتمد على المنفذ المرتبط في جهاز الراوتر والواصل في الشبكة.

٨- يتم الاعتماد على مهندس الشبكة الذي سيقوم بعمل الـ **ACL** وسيقوم بتحديد من المسموح ومن الغير مسموح به.

٩- تقنية الـ **ACL** تعتمد على نوعان من التحديد ، **Deny** , **Premit** سنقوم بتوضيح هذه الأنواع بالتفصيل لنفهم كيف نعمل بهم .

١٠- نستطيع التحديد عن طريق العناوين الخاصة بكل جهاز في الشبكة.

١١- يتم استخدام الـ **WildCard Mask** في عملية الـ **ACL** .

- **يوجد ثلاث أنواع من تقنية الـ ACL :**

1-Standerd , 2- Extended , 3- Name ACL

هذه هي أنواع الـ **ACL** ولكل من هذه الأنواع وظيفته الخاصة سنقوم بشرحها ومعرفة متى نحتاج لكل نوع من هذه الأنواع .

Standerd : هذا النوع يتم استخدامه في حالة نريد منع الشبكة كلها من الوصول إلى شبكة أخرى منعاً كاملاً من دون تحديد ، مثل منع وصول أجهزة الشبكة إلى الشبكة نفسها ومنع خروج الترافك من الراوتر إلى الشبكة بمعنى أنه تم منع الوصول بشكل كامل ومن دون تحديد أي شيء ، ويعتمد هذا النوع في عملية التحديد والمنع على عنوان المرسل **Source IP Address** ، وتبدأ من **1-99** .

Extended : هذا النوع يبدأ استخدامه في حال نريد منع الوصول لخدمة معينة مثل الـ **Web Server** أو ما شابه، في هذا النوع يتم البروتوكول المستخدم ورقم المنفذ التي تعمل عليها الخدمة مثل بروتوكول **http** أو بروتوكول الـ **Telnet** هذا النوع هو من يستطيع منع الوصول لهذه الخدمات، ويعمل هذه النوع مع عناوين المرسل وعناوين المستقبل **Source IP Address** , **Destination IP Address** .

Name ACL : هذا النوع هو الوسيط ما بين الأنواع الأولى فهذا النوع يعتمد على اسم الخدمة أو البروتوكول الذي تريد منع الشبكة من الوصول إليه.

- **طريق التحديد و المنع و السماح في عملية الـ ACL:**

A . B . C . D Address to match 172.16.10.0 0.0.0.255 منع عنوان الشبكة

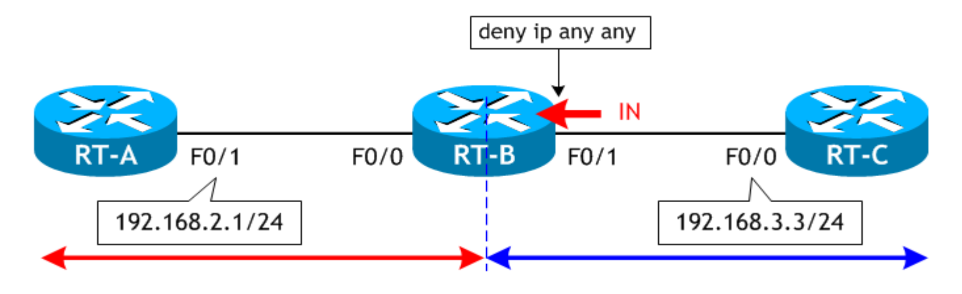
Any Any Source Host Any **منع جميع أجهزة الشبكة**

Host A Single Host Address host 172.16.10.5 **منع جهاز معين**

Deny **أمر منع الوصول**

Premit **أمر سماح الوصول**

ملاحظة مهمة جداً جداً جداً : عندما ا نقوم بعمل منع أو سماح يجب أن نعلم أنه إذا قمنا بعمل منع سيتم المنع على جميع الشبكات ، ويجب أن نرجع لعمل **Premit** للشبكة التي لا نريد عمل منع عليها لنسمح لهم بالدخول .



ACL Configuration

إعدادات الـ ACL

Standard / Extended ACL Configuration



Standard

Router > **enable**

Router # **config t**

Router (config) # **access-list 1 deny host 172.16.10.5**

Router (config) # **access-list 1 permit any**

Router (config) # **interface fastetherent 0/0**

Router (config-if) # **ip access-group 1 out**

Router (config-if) # **exit**

Standard Name ACL

Router > **enable**

Router # **config t**

Router (config) # **ip access-list standard internet**

Router (config-std-nacl) # **deny host 172.16.10.5**

Router (config-std-nacl) # **permit any**

Router (config) # **exit**

Router (config) # **interface fastethernet 0/0**

Router (config-if) # **ip access-group internet out**

Router (config-if) # **exit**



Extended

Router > **enable**

Router # **config t**

Router (config) # **access-list 10 deny host 172.16.10.5 host 192.168.1.1 eq http**

Router (config) # **access-list 10 permit ip any any**

Router (config) # **interface fastetherent 0/0**

Router (config-if) # **ip access-group 10 in**

Router (config-if) # **exit**

Extended Name ACL

Router > **enable**

Router # **config t**

Router (config) # **ip access-list extended http**

Router (config-std-nacl) # **deny tcp host 172.16.10.5 host 192.168.1.1 eq http**

Router (config-std-nacl) # **permit ip any any**

Router (config) # **exit**

Router (config) # **interface fastethernet 0/0**

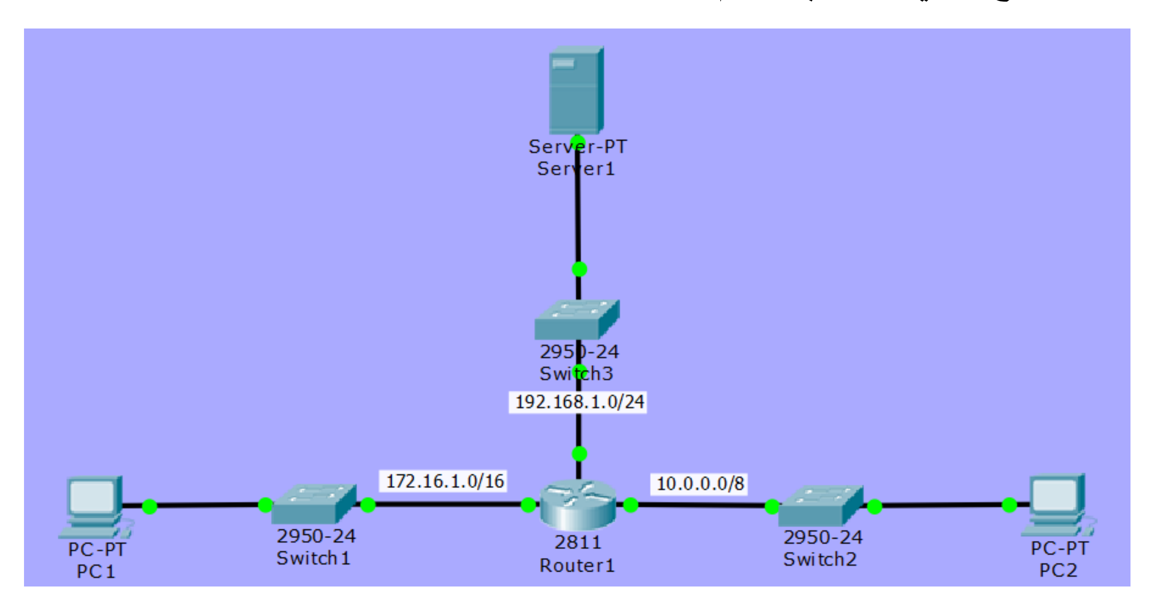
Router (config-if) # **ip access-group 100 in**

Router (config-if) # **exit**

- سنقوم بعمل شبكة مكونة من ثلاث شبكات في مكان واحد ، ونريد أن نقوم بعمل إعدادات الـ **ACL** على أحد الشبكات لنقوم بعمل عدم الوصول إلى شبكة السيرفرات الموجودة في النموذج الذي سنقوم بالتطبيق عليه سنتعرف على إعدادات الشكبات:

- إعدادات الشبكات:

١- الشبكة الأولى بعنوان **192.168.1.0/24** هذه شبكة السيرفرات .
٢- الشبكة الثانية بعنوان **172.16.1.0/16** هذه الشبكة الآخر الخاصة بشبكة الموظفين.
٣- الشبكة الثالثة بعنوان **10.0.0.0/8** هذه الشبكة التي نريد عمل الـ **ACL** عليها ، لكي لا تستطيع الاتصال بشبكة السيرفرات .
٤- النموذج التالي هو الذي سنقوم بعمل التطبيق عليه.



- الآن سنقوم بالدخول على جهاز الراوتر و عمل الإعدادات التالية :

Router > **enable**

Router # **config t**

Router (config) # **access-list 101 deny ip host 10.0.0.2 192.168.1.2 0.0.0.255**

Router (config) # **access-list 101 permit ip any any**

Router (config) # **interface fastEthernet 0/1**

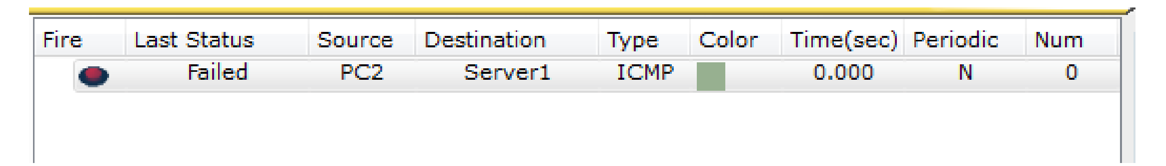
Router (config) # **ip access-group 101 in**

Router (config) # **exit**

Router # **copy running-config startup-config**

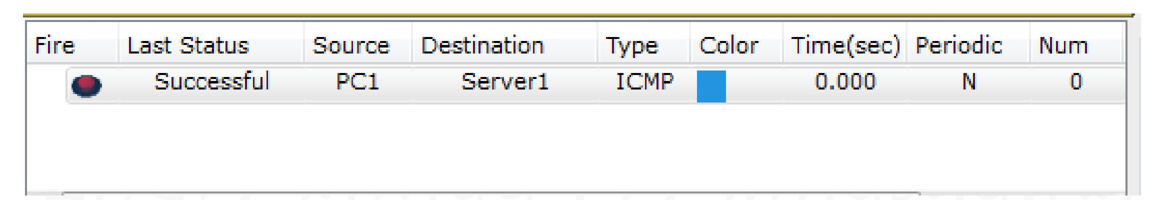
- الأن بهذه الإعدادات قمنا بعمل **ACL** من نوع الـ**Extended** ، ولقد قمنا بمنع الشبكة التي بعنوان **10.0.0.0/8** من الوصول إلى شبكة السيرفرات بينما الشبكة التي بعنوان **192.168.1.0/24** تستطيع الاتصال و الوصول بشبكة السيرفرات بشكل طبيعي جداً.

- نريد أن نقوم بعمل اختبار لنتأكد هل تم منع الشبكة التي بعنوان **10.0.0.0/8** هل تستطيع الوصول أو الاتصال بشبكة السيرفرات أم لا سنقوم بإرسال بكيت ونتأكد .



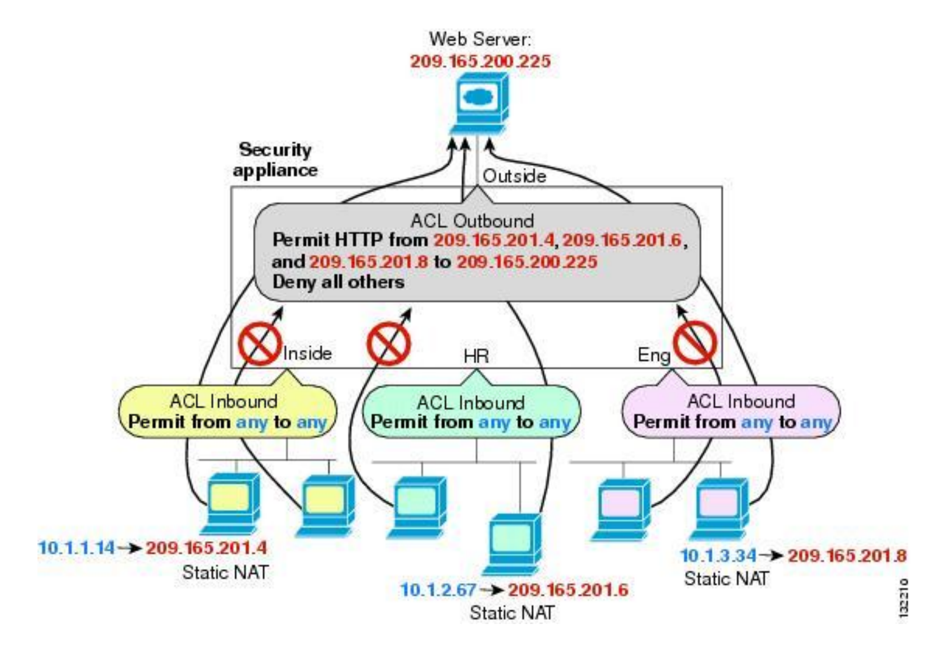
Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num
●	Failed	PC2	Server1	ICMP		0.000	N	0

- لاحظ هذا البكيت تم ارساله من جهاز موجود في شبكة **10.0.0.0/8** إلى شبكة السيرفرات التي تحتوي على عنوان **192.168.1.0/24** ، ولم يستطيع الاتصال أو الوصول إلى الشبكة هذا يدل على أنه تم إعداد عملية الـ **ACL** بنجاح ، ولكن نريد أيضاً أن نتأكد من الشبكة الآخر التي بعنوان **172.16.1.0/16** هل تستطيع الوصول أم لا لنتأكد بنفس الطريق عن طريق ارسال باكيت من الشبكة إلى شبكة السيرفرات.



Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num
●	Successful	PC1	Server1	ICMP		0.000	N	0

- لاحظ أن الباكيت تم إرساله من جهاز موجود في شبكة **172.16.1.0/16** إلى شبكة السيرفرات ، و لقد تم الاتصال ووصول الباكيت بنجاح هذا يدل على أن الشبكة مسموح لها بالدخول إلى شبكة السيرفرات بشكل طبيعي ، ويجب أن نعلم أنه لم نقم بعمل إعدادات الـ **ACL** على هذه الشبكة لقد قمنا فقط على شبكة الـ **10.0.0.0/8** لمنعها من الوصول إلى شبكة السيرفرات .



حماية السويتش Switch Security



Switch Security : لماذا حماية جهاز السويتش أو المبدل لأنه يمثل العمود الفقري للشبكة المحلية وهو الجهاز الذي يربط جميع أجهزة الشبكات مع بعضها البعض في مكان واحد وتكون جميع الأجهزة متصلة بشكل مباشر في نقطة واحدة، ويقوم بتوصيل الأجهزة بمركز البيانات بشكل كامل لهذا السبب يجب أن يكون محمي بشكل كامل من أي عملية اختراق أو عملية هاك وسنتعرف على طرق حماية الجهاز بشكل كامل .

- **خطوات حماية جهاز السويتش :**

يوجد عدة خطوات وعدة طرق لحماية الجهاز سنتعرف على هذه الخطوات بشكل مرتب ومفصل لنستطيع حماية الجهاز بشكل مفهوم.

١- يجب إلغاء عملية التفاوض في منافذ السويتش ، ولقد قمنا بشرح هذه العملية في السابقة دروس السويتش السابقة.

لماذا يجب أن نقوم بعملية إلغاء عملية التفاوض ؟

Trucking Dynamic Protocol (TDP)

يتم استغلال هذه المرحلة في عملية اختراق السويتش مثلاً عندما ا يكون المنفذ متغير يستطيع أي شخص أن يقوم بربط جهاز اللاب توب في منفذ السوتيش ويأخذ حالة المنفذ التي يريدها ويقوم بعدها بعمل فحص وتحليل كل شيء متصل في السويتش وكشف كل عناوين الماك ادرس المخزنة في جهاز السويتش ، ويمكن أيضاً أن يتم استغلال المنفذ مثل ربط جهاز الـ **Hub** ولا ننسى أن جهاز السويتش يقوم بعملية البث المباشر **Broad Cast** في حالة البث المباشر في داخل السويتش سيتم وصول البيانات إلى جهاز الـ **Hub** وجهاز الهاب يكون موصول بجهاز لاب توب بهذه الحالة سيتم كشف كل معلومات الشبكات والعناوين المرسلة والمستقبلة من قبل الشخص الذي قام بربط الهاب بالمنفذ، و هذه من أخطر العمليات التي يجب إغلاقها وعدم ترك المنافذ متغيرة ، وعدم ترك عملية التفاوض تتغير في حالة التوصيل.

إعدادات إلغاء عملية التفاوض في السويتش :

Switch (config) # **interface fastetherent 0/1**

هذا الأمر لتحديد منفذ واحد فقط لتطبيق عملية منع التفاوض عليه

Switch (config) # **interface fastetherent 0/1-10**

هذا الأمر لتحديد مجموعة من المنافذ وتطبيق عملية منع التفاوض

Switch (config-if-range) # **switchport mode trunk**

هذا الأمر لتطبيق أمر عملية منع التفاوض على منافذ الـ **Trunk** بمعنى أن المنافذ التي تعمل في حالة الـ **Trunk** فقط لا غير سيتم تجهيز المنفذ ليعمل **Trunk** فقط لا غير.

و بنفس الأمر نقوم بعمل باقي الحالات مثل :

Switch (config-if-range) # **switchport mode access**

Switch (config-if-range) # **switchport nonegotiate**

٢- يجب تحديد عدد الأجهزة الموجودة في الشبكة والأجهزة المتصلة فقط في السويتش والمسموح لها الاتصال بالمنافذ فقط ، مثلاً نريد تحديد جهاز حاسوب معين هو من يستطيع الاتصال بأحد المنافذ في السويتش بعد أن نقوم بتحديد عنوان الماك ادرس الخاص بالجهاز المطلوب ، وهذه العملية تسمى **Port Security** .

Switch (config) # **interface fastethernet 0/10**

تحديد المنفذ

Switch (config-if) # **switchport port-security maximum 1**

تحديد عدد المنافذ التي نريد تطبيق الحماية عليها

Switch (config-if) # **switchport port-security mac-address ?**

تحديد عنوان الماك ادرس للأجهزة المتصلة في المنافذ

Switch (config-if) # **switchport port-security violation ?**

تقرير حالة المنفذ في حالة تم فصل أو تركيب جهاز غير الجهاز المعين

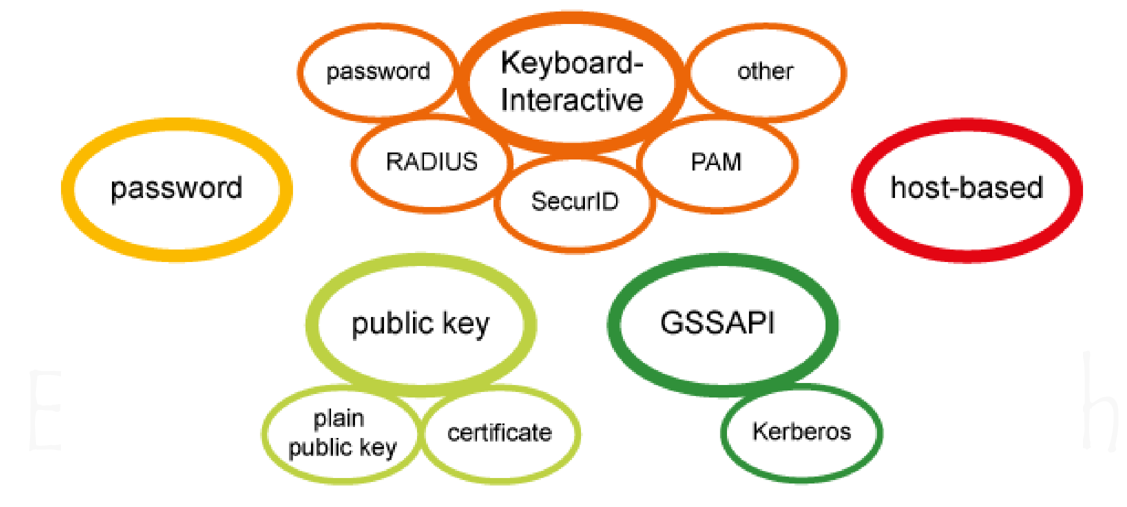
٣- يجب إغلاق المنافذ التي لم يتم استعمالها ونقلها لشبكة **Vlan** غير مفعلة لكي لا يتم استغلال هذه المنافذ في عملية ربط جهاز خارج الشبكة، مثلاً عندما ا يكون منفذ مفعل ويعمل من الطبيعي جداً أن يتم ربط أي جهاز حاسوب مثل اللاب توب فيه ومراقبة الشبكة بأكثر من طريق ، مع العلم أن هذا ما يبحث عنه المخترقين.

٤- يجب أن تقوم بعمل إعدادات كلمات المرور على السويتش بشكل عام، على جميع السويتشات نقوم بتشفير كلمة المرور أيضاً .

٥- يجب عدم استخدام شبكة الـ **Vlan 1** الموجودة في السويتش ، لأنها قد تكون أخطر شبكة في السويتش لأنها الرئيسية في السويتش ويفضل عدم استخدامها وأن نقوم بعمل **Vlan** أخرى وإضافة الأجهزة عليها.

٦- عليك أن تقوم بعمل شبكة **Vlan** في السويتش وتوزيع جميع المنافذ على الـ**Vlan** على حسب تقسيم الشبكة لديك ويفضل أيضاً أن تقوم بعمل **Vlan** غير مستعملة للمنافذ الغير مستعمله أيضاً ونقل هذه المنافذ إلى الـ **Vlan** الغير مستعملة.

طرق التحقق Authentication Methods



Authentication : هي عبارة عن عملية التحقق من المتصلين بالشبكة أو من يريد الاتصال بالشبكة، ويجب قبل الدخول أو الاتصال بالشبكة أو الاتصال بأحد أجهزة الشبكة مثل السيرفرات أن يقوم بالتعريف عن نفسه وبعدها يبدأ نظام الحماية بتأكيد من هل المتصل مصرح له بالدخول أم لا وتتم هذه العملية على مراحل مهمة جداً يجب أن نعرفها .

١- يجب على المتصل أن يؤكد على المعلومات المسموح بها للدخول إلى الشبكة **Something You Know** .

٢- يجب أن يكون لدى الشخص الذي يريد الاتصال بالشبكة معلومات وصلاحيات ما قبل دخوله للشبكة **Something You have** .

٣- في بعض الشركات يتم الاعتماد على الشهادة الرقمية وهذه الشهادة تكون موثوقة بشكل كبير جداً ويكون لديها تاريخ إصدار وتاريخ انتهاء **Certifcate Authority** .

٤- يوجد بروتوكولات مخصصة في مجال الحماية مثل بروتوكول الـ **CHAP** الذي يقوم بعملية التشفير ما بين عملية الاتصال ما بين السيرفر والمستخدم أو المضيف .

٥- يوجد بروتوكول الـ **Kerberos** هذا البروتوكول من أهم البروتوكولات في مجال مايكرسوفوت ، وظيفة هذا البروتوكول القيام بعمل تذكرة **Tickets** لكل مستخدم و يقوم بتخزين هذه التذكرة في السيرفر فعندما ا يريد المستخدم الاتصال بالسيرفر سيتم طلب التذكرة منه ويبدأ بروتوكول الـ **Kerberos** بإرسال الطلب إلى السيرفر ليتأكد هل المستخدم هذا موجود أم لا.

٦- يوجد أيضاً بروتوكول الـ **PAP** هذا البروتوكول ضعيف بعض الشيء لأنه فقط يعتمد على اسم المستخدم و كلمة المرور ، بمعنى أنه من السهل اختراق وفك تشفير هذا النوع من الأمن على عكس بروتوكول الـ **Kerberos** .

أمن الشبكات

Network security



أمن شبكات المعلومات الإلكترونية : إن فكرة نقل المعلومات وتبادلها عبر شبكة ليست بفكرة جديدة ابتدعها العصر الحالي بل إنها فكرة قديمة ولعل من أقرب شبكات المعلومات التي عاشت عصوراً طويلة، وما تزال تتواجد في العصر الحالي : شبكات البريد ،وشبكات توزيع الكتب والصحف ،الجرائد والمجلات .في القرن التاسع عشر تمكن الإنسان من نقل المعلومات سلكياً ثم لاسلكيا .وفي ذات القرن ظهرت الأنظمة الهاتفية ،وأصبح نقل الصوت آنياً ، وبالتالي التخاطب أيضاً ،عبر مسافات بعيدة أمراً ممكناً ثم تطورت الشبكات شيئا فشيئا إلى أن أصبحت في صورتها الحالية.

أمن شبكات المعلومات: هي مجموعة من الإجراءات التي يمكن خلالها توفير الحماية القصوى للمعلومات والبيانات في الشبكات من كافة المخاطر التي تتهددها، وذلك من خلال توفير الأدوات والوسائل اللازم توفيرها لحماية المعلومات من المخاطر الداخلية أو الخارجية.

تصنيف جرائم المعلومات

جرائم تهدف لنشر المعلومات : يتم نشر معلومات سرية تم الحصول عليها بطرق غير مشروعة عن طريق الاختراقات لشبكات المعلومات ونشر هذه المعلومات

جرائم تهدف لترويج الإشاعات. وهنا يتم نشر معلومات مغلوطة وغير صحيحة تتعلق بالأشخاص أو المعتقدات أو الدول بهدف تكدير السلم العام في البلدان، وكذلك نشر الإشاعات عن بعض الأشياء وإحداث البلبلة في المجتمعات.

جرائم التزوير الإلكترونية. وهنا يتم استخدام وسائل التكنولوجيا في عمليات التزوير بغرض تحقيق هدف معين، وكذلك يندرج تحتها عمليات التحويل المصرفي الوهمية من حسابات إلى أخرى عن طريق اختراق شبكات المصارف.

جرائم تقنية المعلومات. وأهم مثال لها هو عمليات القرصنة التي تحدث للبرامج الحاسوبية الأصلية والتي يتم عمل نسخ منها لتباع في الأسواق بدلاً من النسخ الأصلية.

مكونات أمن شبكات المعلومات :

سرية المعلومات Data Confidentiality : وهذا الجانب يشتمل على الإجراءات والتدابير اللازمة لمنع إطلاع غير المصرح لهم على المعلومات التي يطبق عليها بند السرية أو المعلومات الحساسة، وهذا هو المقصود بأمن وسرية المعلومات، وطبعاً درجة هذه السرية ونوع المعلومات يختلف من مكان لآخر وفق السياسة المتبعة في المكان نفسه، ومن أمثلة هذه المعلومات التي يجب سريتها: المعلومات الشخصية للأفراد.

سلامة المعلومات Data Integrity : في هذا الجانب لا يكون الهم الأكبر هو الحفاظ على سرية المعلومات وإنما يكون الحفاظ على سلامة هذه المعلومات من التزوير والتغيير بعد إعلانها على الملأ، فقد تقوم هيئة ما بالإعلان عن معلومات مالية أو غيرها تخص الهيئة وهنا يأتي دور الحفاظ على السلامة بأن تكون هذه المعلومات محمية من التغيير أو التزوير، ومن أمثلة ذلك مثلاً: إعلان الوزارات أو الجامعات عن أسماء المقبولين للعمل بها، تتمثل حماية هذه القوائم في أن تكون مؤمنة ضد التغيير والتزوير فيها بحذف أسماء ووضع أسماء غيرها مما يسبب الحرج والمشكلات القانونية للمؤسسات، وأيضاً بالنسبة للمعلومات المالية بتغيير مبلغ مالي من **100** إلى **1000000** وهذا هام جداً لما يترتب عليه من خسائر فادحة في الأموال.

ضمان الوصول إلى المعلومات Availability: لعله من المنطقي أن نعرف أن كل إجراءات وصناعة المعلومات في الأساس تهدف إلى هدف واحد وهو إيصال المعلومات والبيانات إلى الأشخاص المناسبين في الوقت المناسب، وبالتالي فإن الحفاظ على سرية المعلومات وضمان سلامتها وعدم التغيير فيها لا يعني شيئاً إذا لم يستطع الأشخاص المخولين أو المصرح لهم الوصول إليها، وهنا تأتي أهمية الجانب الثالث من جوانب أو مكونات أمن المعلومات وهو ضمان وصول المعلومات إلى الأشخاص المصرح لهم بالوصول إليها من خلال توفير القنوات والوسائل الآمنة والسريعة للحصول على تلك المعلومات، وفي هذا الجانب يعمل المخربون بوسائل شتى لحرمان ومنع المستفيدين من الوصول إلى المعلومات مثل حذف المعلومات قبل الوصول إليها أو حتى مهاجمة أجهزة تخزين المعلومات وتدميرها أو على الأقل تخريبها.

جدار الحماية , Firewall



جدار الحماية Firewall : يشار إليه في بعض الأحيان بعبارة الجدار الناري ، هو جهاز و/أو برنامج يفصل بين المناطق الموثوق بها في شبكات الحاسوب، ويكون أداة مخصصة أو برنامج على جهاز حاسوب آخر، الذي بدوره يقوم بمراقبة العمليات التي تمر بالشبكة ويرفض أو يسمح فقط بمرور برنامج طبقاً لقواعد معينة.

و كما نعلم ايضاً سيسكو تقوم بعمل أجهزة جدار الحماية و يوجد أكثر من نوع لهذه الاجهزة الخاصة في شركة سيسكو ، ولكن في هذا الدرس سنقوم بشرح الجدار الناري بشكل عام لنتعرف عليه ؟

وظيفة جدار الحماية : وظيفة جدار الحماية الأساسية هي تنظيم بعض تدفق حزمة الشبكة بين شبكات الحاسوب المكونة من مناطق ثقة المتعددة. ومن الأمثلة على هذا النوع الإنترنت التي تعتبر منطقة غير موثوق بها- وأيضا شبكة داخلية ذات ثقة أعلى ، ومنطقة ذات مستوى ثقة متوسطة، متمركزة بين الإنترنت والشبكة الداخلية الموثوق بها، تدعى عادة بالمنطقة منزوعة.

وظيفة جدار الحماية من داخل الشبكة هو مشابه إلى أبواب الحريق في تركيب المباني. في الحالة الأولى يستعمل في منع اختراق الشبكة الخاصة، وفي الحالة الثانية يعطل دخول الحريق من منطقة (خارجية) إلى بهو أو غرفة داخلية.

من دون الإعداد الملائم فإنه غالباً ما يصبح الجدار الناري عديم الفائدة. فممارسات الأمان المعيارية تحكم بما يسمى بمجموعة قوانين المنع أولاً جدار الحماية، الذي من خلاله يسمح بمرور وصلات الشبكة المسموح بها بشكل تخصيصي فحسب. ولسوء الحظ، فإن إعداد مثل هذا يستلزم فهم مفصل لتطبيقات الشبكة ونقاط النهاية اللازمة للعمل اليومي للمنظمات. العديد من أماكن العمل ينقصهم مثل هذا الفهم وبالتالي يطبقون مجموعة قوانين "السماح أولاً"، الذي من خلاله يسمح بكل البيانات بالمرور إلى الشبكة ان لم تكن محددة بالمنع مسبقاً.

مرشحات العبوة Packet Filters :

أول بحث نشر عن تقنية الجدار الناري كانت عام **1988**، عندما ا قام مهندسون من(**DEC**) بتطوير نظام مرشح عرف باسم جدار النار بنظام فلترة العبوة، هذا النظام الأساسي يمثل الجيل الأول الذي سوف يصبح عالي التطور في مستقبل أنظمة أمان الإنترنت. في مختبرات **AT&T** قام بيل شيزويك وستيف بيلوفين بمتابعة الأبحاث على ترشيح العبوات وطوروا نسخة عاملة مخصصة لشركتهم معتمدة على التركيبة الأصلية للجيل الأول.

تعمل فلترة العبوات بالتحقق من العبوات (**packets**) التي تمثل الوحدة الأساسية المخصصة لنقل البيانات بين الحواسيب على الإنترنت. إذا كانت العبوة تطابق مجموعة شروطات مرشح العبوة ، فإن النظام سيسمح بمرور العبوة أو يرفضها (يتخلص منها ويقوم بإرسال اشارة "خطأ" للمصدر.

هذا النظام من مرشحات العبوات لا يعير اهتماما إلى كون العبوة جزءاً من تيار المعلومات لا يخزن معلومات عن حالة الاتصال

وبالمقابل فإنه يرشح هذه العبوات بناءً على المعلومات المختزنة في العبوة نفسها في الغالب يستخدم توليفة من مصدر العبوة المكان الذاهبة إليه، النظام المتبع، ورقم المرفأ المخصص لـ (**UDP**) (**TCP**) الذي يشمل معظم تواصل الإنترنت.

لأن (**TCP**) و (**UDP**) في العادة تستخدم مرافئ معروفة إلى أنواع معينة من قنوات المرور، فإن فلتر عبوة "عديم الحالة" يمكن أن تميز وتتحكم بهذه الأنواع من القنوات (مثل تصفح المواقع، الطباعة البعيدة المدى، إرسال البريد الإلكتروني، إرسال الملفات، إلا إذا كانت الأجهزة على جانبي فلتر العبوة يستخدمان نفس المرافئ الغير اعتيادية.

فلتر محدد الحالة Stateful Filters : هنا يقوم جدار الحماية بمراقبة حقول معينة في المظروف الإلكتروني، ويقارنها بالحقول المناظرة لها في المظاريف الآخر التي في السياق نفسه، ونعني بالسياق هنا مجموعة المظاريف الإلكترنية المتبادلة عبر شبكة الإنترنات بين جهازين لتنفيذ عملية ما. وتجري غربلة المظاريف التي تنتمي لسياق معين إذا لم تلتزم بقواعده: لأن هذا دليل على أنها زرعت في السياق وليست جزءا منه، مما يثير الشكوك بأنها برامج مسيئة أو مظاريف أرسلها متطفل.

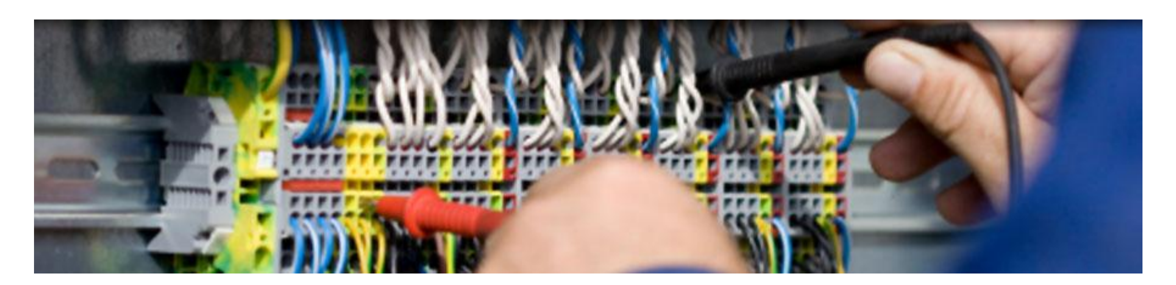
طبقات التطبيقات (Application Layer Firewall) :

بعض المنشورات بقلم جين سبافورد من جامعة بوردو، بيل شيزويك من مختبرات **AT&T**، وماركوس رانوم شرحت جيلاً ثالثاً من الجدارن النارية عرف باسم "الجدار الناري لطبقات التطبيقات (**Application Layer Firewall**) ، وعرف أيضا بالجدار الناري المعتمد على الخادم النيابي (**Proxy server**) وعمل ماركوس رانوم قاد ابتكار أول نسخة تجارية من المنتج قامت **DEC** بإطلاق المنتج تحت اسم **SEAL** .

فهرس المستوى السادس استكشاف المشاكل و حلها في الشبكة

Troubleshooting

استكشاف المشاكل و حلها في الشبكة



استكشاف المشاكل و حلها في الشبكة : هي عبارة عن عملية استكشاف يقوم فيه مهندس الشبكة في حالة حدوث مشكلة في الشبكة ، و تبداء هذه العملية بكثير من الحلول التي يبداء في التفكير بها للوصول لحل المشكلة و من أهم المواضيع التي يجب أن يكون مهندس الشبكة على معرفة بها هي الفهم الجيد للشبكة التي يقيم عليه في العمل أو في الشركة ، ويجب أن يكون على معرفة كاملة بكل تفاصيل الشبكة اما في حالة لا يعرف اية تفاصيل أو اية معلومات عن الشبكة يجب عليه أن يبداء بتفكير كيف يقوم بعملية استكشاف الخلال أو العطل في الشبكة ويجب أن يكون على معرفة كامل و ممتازة في نموذج تكوين و ارسال البيانات الـ **OSI** ليستطيع تحليل المشكلة و يجب أن يكون على معرفة في ، أوامر استكشاف جداول التوجيه و الاوامر الآخر التي قمت بشرحها في الدورس السابقة مثل أمر الـ **Show** من أهم الاوامر المستخدمة في عملية استكشاف الاخطاء ، وبجب أن يكون على فهم جيد أو ممتاز ليستطيع أن يقوم بعملية اصلاح الاخطاء في الشبكة ، ويوجد بعض المواضيع التي ساقوم بذكره و شرحها في عملية استكشاف الاخطاء .

- يجب أن يكون مهندس الشبكة الناجح و المميز أن يكون على معرفة بشكل كامل في المواضيع التالية ليستطيع حل المشاكل و التعامل معها في حال تم وجود خطاء .

١- **OSI** يجب أن يكون على معرفة كاملة في نموذج الاتصال و معرفة كل طبقة ماذا يعمل به و معرفة كل طبقة ما هي وظيفتها بالتفصيل الممل .
٢- **TCP/IP** يجب فهم النموذج المطور من الـ **OSI** .
٣- يجب معرفة و فهم البروتوكولات و كيفها تعمل و كيفها تتم عملية الإعدادات و خصوصي بروتوكولات التوجيه .
٤- يجب أن يكون لديك خطة ما قبل البداية في العمل مثل معرفة بعض المعلومات ما قبل حدوث المشكلة ، لنتمكن وصول الحل بسرعة .
٥- يجب على مهندس الشبكة أن يكون على اطلع كامل و بشكل منظم لمراقبة الشبكة ، مثل ما قبل حدوث المشكلة أو وقوع الخطاء يكون على معرفة .
٦- يجب أن يكون على معرفة كاملة و العمل بشكل ممتاز على البرامج التي تعمل على عملية الاصلاح مثل برامج التالية :

Backup , SNMP , Syslog , Wire shark , NetFlow

- سنبداء الأن بتعرف على عملية اكتشاف الاخطاء عن طريق نموذج الاتصال الـ OSI

طبقات الأتصال مكونه من سبعة طبقات و كل طبقة له و وظيفتها الخاصة بها حيث يتم بناء الدتا بشكل التالي اذا كانت من جهة المرسل ، ستبداء بنزول في الطبقات لحتى الوصول الى البطقة الاولى ، اما من جهة المستقبل سيتم بناء الدتا من اسفل الى اعلى هذا الشكل الطبيعي لتكوين الدتا ولكن في حال تم وجود مشكلة في احد الطبقات كيف نعرف في اية طبقة من هذه البطقات السبعة ، سنبداء في التعرف على بعض المشاكل .

Services
POTS, X.25, ISDN, T1, T1C, T3, ADSL
T1, T3, Elect. and Opt., SONET / SDH, Ethernet
Elect. and Opt., SONET / SDH, Ethernet
POTS, T1, T3, xDSL, VoIP, IPTV, Ethernet
VoIP, IPTV, Ethernet
Cellular Voice, SMS, MMS, Ethernet

Application
Presentation
Session
Transport
Network
Data Link
Physical

TABS, TBOS, Other
TL1
CMIP, CMISE, ACSE, ROSE, SMASE, FTAM
BER, ASN.1
Session V.2
SNMP, DNS, FTP, LDAP, LMP, NTP, SSH, rLogin, Telnet, CORBA, PKI, PKCS (RSA), SIP, SOAP
HTTP, DHCP, OpenVPN, SMTP, POP3, IMAP, MIME, TLS / SSL, WAE / WAP
CM, MM, BSTM, RRM
MAP
ITOT
TP4
TCP, UDP, RIP, BGP
GMPLS RSVP-TE
SCCP, NSP, MTP, (SS7)
PLP (X.25)
TARP
CLNS, SNDCF, ES-IS, IS-IS, NSAP
IPv4, IPv6, IPSec, ICMP, OSPF
MPLS, LDP, GMPLS CR-LDP
LAP, SLIP
LAPB, PPP
HDLC, LAPD, CSMA/CD
GFP, FEC
ATM Adaption (AAL 1, 3/4, 5), ATM Layer
LLC, CSMA/CD, ARP, RARP, RSTP, MSTP, L2TP, VLAN, LAPD, PPP, PPPOE, MAC
LAPD, LAPDm
DS0 thru 5, E0 thru 5, SF, ESF, ISDN, 2-wire TR, ADSL, RS-232, RS-422, Modem (Bell, V.)
VT-n, C-n VC-n, TU-n, TUG-n, STS-n, AU-n, OC-n, STM-n, SDCC, LDCC, LAN
ODU0, 1, 2, 2e, OTU1, 2, 2e, 3, 4, GCC, MP, SONET, SDH, Ethernet, FC
ATM PHY, UNI, NNI, PDH, SONET, SDH, Ethernet, xDSL, 2-wire TR
UNI, NNI, LAN-PHY, WAN-PHY, 10Base-T, 100Base-TX, 1000Base-T, 1000Base-X
WEP, WPA, Wi-Fi
GPRS, UMTS, HSPA, GSM, LTE, A, Abis, UM

ITU-T OSI Model | PDH | SONET / SDH | OTN / ASON / ASTN | ATM | MPLS / T-MPLS | Ethernet | Cellular

Legacy | Metro Core & Long Haul – Backbone | Metro Edge & Metro Core – Access | Wireless Access

هذا نموذج مفصل بالتفصيل الممل لو نظرنا عليه سنجد انه كل بطقة من الطبقات تدعم انواع مختلفة من البروتوكولات و سنبداء بفهم النموذج بشكل ممتاز لنستطيع حل المشاكل بكل بساطة .

١ـ الطبقة السابعة و هي طبقة الـ **Application** و هي التي تدعم البرامج و التطبيقات ، مثل لو قمنا بدخول على برنامج الاتصال عن بعد الـ **Remote Control** و وجدنا انه لا يعمل يجب أن نعلم انه هذه المشكلة في الطبقة السابعة من نموذج الاتصال و لا ننسى أن هذه البرنامج وظيفته الاتصال عن بعد عن طريق الشبكة و الحل هنا يجب عمل فحص للبرنامج و التاكد من سلامة تنصيبه و عدم فقدان اية ملف من ملفات هذا البرنامج.

٢- الطبقة السادسة **Presentation** و وظيفة هذه الطبقة تحديد نوع البيانات المرسلة ، و تقوم ايضاً بضغط البيانات و فكها مثل عندما نقوم بتحميل أحد الملفات من الانترنت سنجد تم نزوله على النظام ولكن غير مكتلم و يكون شكل الملف غير معرفو لي انه لم يتم اكمل الملف و هو قيد التحميل من الانترنت ، ولكن عند اكتمال البرنامج ستجد أن البرنامج لقد اخذ الصيغة التي يجب ان يكون بها بشكل طبيعي ، و في حال لما يكتمل و تم فصل التحميل هنا ستظهر مشكلة و يجب أن نعرف انه هذه المشكلة في الطبقة السادسة لي انه البرنامج لم يكتمل تحميله بشكل صحيح .

٣- الطبقة الخامسة **Session** وهي الطبقة المسؤولة عن الاتصال و فتح قنوات لربط الاتصال ، و في حالة انه يوجد خطاء أو عطل في عملية الاتصال يجب عليك أن تعلم أن هذه المشكلة في طبقة الـ **Session** لي انه هي المسؤولة عن فتح قنوات و مسارات الاتصالات ، مثل عندما نريد فتح أكثر من موقع في نفس الوقت هذه الطبقة هي التي تقوم بتنسيق و تنظيم عملية الاتصال و فتح المنافذ .

٤- الطبقة الرابعة **Transport** هذه الطبقة المخصصة لنقل الداتا و يعم فيها أهم بروتوكولات النقل مثل **UDP** , **TCP** حيث عندما انتا تقوم بتحميل أحد البرامج من الانترنت أو تقوم بنقل برانامج و يفشل يجب أن تعرف أن الخطاء في الطبقة الرابعة لي انه هي المسؤولة عن عملية النقل و تضم تحتها الكثير من البروتوكولات مثل **FTP** , **TFTP** و الكثير من بروتوكولات النقل .

٥- الطبقة الثالثة **Network** و هي الطبقة المسؤولة عن الشبكات و اتصال الشبكة في بعضها البعض و تحويل البكت ما بين المسارات ، و في حال انه يوجد أحد المسارات أو البكت تسلك مسار و عنوان معين يجب أن نبداء بتحليل و العمل في الطبقة الثالثة لي انه هي المسؤولة عن الشبكات و كل ما يتعلق في بروتوكولات الشبكة .

٦- الطبقة الثانية **Data Link** و هي المسؤولة عن الفريم أو الاطار و يجب أن تعلم أن اية اخطاء أو اية خلال في كرت الشبكة أو في الماك ادرس يجب أن تبداء بتفكير في طبقة الـ **Data Link** لي انه هي المسؤولة عن هذه الوظيفة .

٧- الطبقة الاولى و هي الطبقة الفيزيائية **Physical** و هي التي تعمل على نقل البيانات بشكل صفر واحد بعد وصولها الى هذه الطبقة سيتم ارسال البيانات في الكابل و عندما ا لا يوجد اية ارسال أو اية استقبال ، يجب أن نبداء بفحص الكابل و لي انه هو اول رابط في الشبكة .

- الأن بعد أن فهمنا كيف سيتم تحليل المشاكل و استكشافها يجب أن تكون على معرفة ممتاز في هذه الطبقة و مراجعة دورية لتستطيع أكتشاف المشكل في أسرع وقت ممكن

، و يجب أن تكون على بحث مستمر عن الاعطال و المشاكل التي تحدث في الشبكات
.

- **المشاكل الفيزيائية و حلها في الشبكة :**

يوجد أوامر مهم جداً يجب أن نكون على معرفة فيها في عملية استكشاف المشاكل مثل نريد معرفة إعدادات الراوترات و المنافذ .

Router # **show controllers serial 0/0/0**

هذا أمر لعرض ملف إعدادات منافذ السيريل حيث يكون في هذا الملف كثير من المعلومات بخصوص منفذ السيريل .

Router # **show ip interface brief**

هذا أمر مهم جداً جداً و وظيفة هذا الامر انه يقوم بعرض اعدادات المنافذ بشكل مرتب و مفصل .

Router # **show running-config**

هذا الامر لعرض ملف الاعدادات الذي يعمل في الوقت الحالي في الرام و هي الذاكرة المؤقته و يحتوي هذا الملف على كثير من المعلومات و الاعدادات المهم جداً فهو يعطي تفصيل كامل عن الاعدادات التي تعمل على الراوتر .

- **مشاكل الشبكة الوهمية الافتراضية Vlan Problems :**

يوجد ايضاً بعض الاوامر المستخدمة في استكشاف مشاكل الشبكة الوهمية سنتعرف عليها.

Switch # **show van**

هذا الامر لعرض شبكات الـ **Vlan** كلها التي تتوجد في داخل السويتش بشكل كامل مع تفاصيل كل شبكة .

Switch # **show interfaces trunk**

هذا الامر لعرض المنافذ التي تعمل بحالة الـ Trunk مع عرض التفاصيل .

Switch # **show vtp status**

هذا الامر لعرض حالة بروتوكول الـ **VTP** بشكل مفصل مع المعلومات و الاعدادات .

Switch (config) # **no spanning-tree vlan 1,2,3,4**

هذا الامر مهم و خطير في نفس الوقت و وظيفته انه يقوم بعملية الغاء بروتوكول الـ **STP** ما بين شبكات الـ **Vlan** التي نريدها .

Switch (config) # **interface fastetherent 0/5**

Switch (config-if) # **spanning-tree portfast**

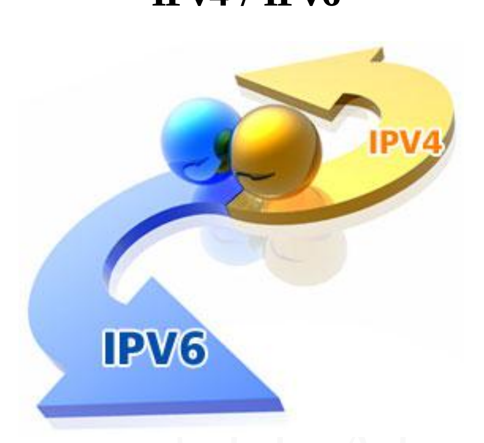
هذا الامر لتحديد منفذ معين و تطبيق خاصية الـ **Portfast** عليه .

Switch # **show spanning-tree**

هذا الامر لعرض اعدادات بروتوكول الـ **STP** .

مشاكل العناوين المنطقية في الشبكة المحلية

IPv4 / IPv6



مشاكل العنوان في الشبكة تعتبر من المشاكل المتكررة بشكل مستمر في حال عدم وجود خادم يقوم بتوزيع العناوين ، وحتى ولو تم وجود خادم يقوم بتوزيع العناوين من الممكن و الطبيعي أن يحد تصادم و تكرار في العناوين، مثل جهاز ياخذ عنوان جهاز آخر في موجود في الشبكة مما يحدث تصادم في العناوين و عدم التميز ما بين العناوين سنتعرف على كيفية حل هذه المشكلة .

١- يجب أن تقوم بعمل خطة ما قبل البداء في العمل مثل معرفة بداية العناوين ستبداء من أين و تنتهي الى أين لنستطيع فهم الشبكة و معرفة ترتيب العناوين .
٢- يجب أن لا يتكرار العناون الواحد في داخل الشبكة على نفس الاجهزة لعدم التصادم و عدم التفرقه في داخل الشبكة ما بين الجهازين الذين حاصلين على نفس العنوان .
٣- عندما ا يتكرار العناون في داخل الشبكة سيتم اظهر رسالة تقول لك انه هذا العنوان مستخدم من قبل جهاز آخر على الشبكة .
٤- يوجد بعض مشاكل الشبكة انه مهندس الشبكة أو الموظف يقوم بوضع عنوان منطقي مختلف عن العنوان المنطقي الآخر ، مع العلم انهم متصلين في نفس الشبكة و بنفس جهاز السويتش ولكن يكون العنوان مختلف ويجب اعادة ترتيبه ليكون بنفس العنوان .
٥- تقسيم الشبكة الخطاء مثل عندما ا نقوم بتقسيم الشبكة و نقوم بتوزيع العناوين يجب أن تكون جميع الاجهزة التي تاخذ نفس العنوان أن تاخذ نفس عنوان الشبكة **Subnet Mask** ، اما اذا لم يتم وضع نفس القناع لان تعمل الاجهزة مع بعضها البعض .

٦- يجب أن يكون عنوان البوابة الخارجية التي توصلنا في شبكة الانترنت صحيح ، مثل اذا كان **192.168.1.1** يجب أن تكون جميع الاجهزة في داخل الشبكة تاخذ هذا العناون لتستطيع الاتصال بشبكة الانترنت .
٧- خادم توزيع العناوين بشكل تلقائي و هو الـ **DHCP** يوجد اكثر من مشكلة من الممكن أن نقع فيها مثل :

- من المشاكل الكثيرة التي تحدث في سيرفر الـ **DHCP** مشكلة نفاذ العناوين بمنعى انه تم توزيع كل العناوين على الاجهزة في هذه الحالة ، هذه مشكلة و يجب أن نقوم بحلها و اول تفكير يجب أن تفكر فيه في حل هذه المشكلة أن تقوم بعمل **Pool** جديدة أو تقوم بتقسيم العناوين أو على طبيعية الشبكة لديك و هذا الامر يعود لك عن بنية الشبكة .

- من الممكن أن يكون مهندس الشبكة الذي يكون قليل الخبرة بعمل إعدادات خطاء في عملية بناء سيرفر الخدمة الـ **DHCP** و على مهندس الشبكة ذو الخبرة العالية معالجة هذا الامر ، و يفضل عدم الدخول في عملية استكشاف اخطاء الـ **DHCP** اذا لم يكن لديك خبرة كافية في هذه الخدمة .

- من المشاكل الكبيرة جداً في الشبكة أن يتوجد راوتر ما بين شبكة الخوادم و شبكة المستخدمين ، هذه من أكبر المشاكل لي انه سيرفر الـ **DHCP** يعمل على البث المباشر لتوزيع العناوين و كما نعلم جهاز الراوتر يقوم بكسر البث المباشر في هذه الحالة لان يستطيع سيرفر الخدمة توزيع العناوين لشبكة المستخدمين و لا المستخدمين يستطيعون طلب العناوين من سيرفر الخدمة الـ **DHCP** في هذه الحالة الحل هو أن تقوم بعمل **DHCP Realy Agent** ، هذه الخدمة وظيفتها تمرير البث المباشر فقط لخدمة الـ **DHCP** ليتسطيع توزيع العناوين على الشبكة .

- من أهم المشاكل التي تحصل في سيرفر خدمة الـ **DHCP** هي نفاذ كل العناوين وذلك لوجود أجهزة متحركة مثل جهاز الاب توب أو الجوال تخاذ عنوان من الـ **DHCP** و تذهب و يبقى العنوان محجوز في السيرفر ولن يتم توزيعها لفتره معينها ، لذالك يجب على مهندس الشبكة أن يكون على معرفة فيها ليستطيع تجب هذه المشكله و حل هذه المشكلة أن تقوم بعمل إعداد لهذه الاجهزة المحموله مثل عندما ياخذ الجهاز عنوان و يذهب و مضى على هذا العنوان وقت زماني و الجهاز غير متصل سيتم ارجاع العنوان على الـ **Pool** ليقوم بتوزيعه من جديد .

مشاكل و حلول الـ ACL - Access List

Router # **show access-lists** / Router # **show ip access-lists**

Router # **show ip interface**

الاوامر السابقة من أهم الاوامر التي يجب أن يكون مهندس الشبكة على معرفة فيها ليستطيع عرض حالة الـ **ACL** و معرفة الاعدادات و تحليل سبب المشكلة .

عملية استكشاف مشاكل البروتوكولات في الشبكة



- **أوامر أستكشاف أخطاء و إعدادات بروتوكول الـ NAT :**

Router # **show running-config**

Router # **show ip nat translations**

- **أوامر استشكاف أخطاء إعدادات التوجيه اليدوي Static Routing :**

Router # **show ip route**

Router # **show ipv6 route**

Router # **ping**

Router # **traceroute**

- **أوامر استشكاف أخطاء إعدادات التوجيه الديناميكي Dynamic Routing :**

RIP Trobleshooting

Router # **show ip route**

Router # **show ipv6 route**

Router # **show running-config**

Router # **ping**

Router # **traceroute**

Router # **show ip route**

OSPF Trobleshooting

Router # **show ip route**

Router # **show ipv6 route**

Router # **show ip ospf database**

Router # **show ipv6 ospf database**

Router # **show ip ospf neighbor**

Router # **show ipv6 ospf neighbor**

Router # **show running-config**

Router # **ping**

Router # **traceroute**

EIGRP Trobleshooting

Router # **show ip route**

Router # **show ipv6 route**

Router # **show ip eigrp database**

Router # **show ipv6 eigrp database**

Router # **show ipv6 eigrp neighbor**

Router # **show running-config**

Router # **ping**

Router # **traceroute**

Simple Network Management Protocol (SNMP)



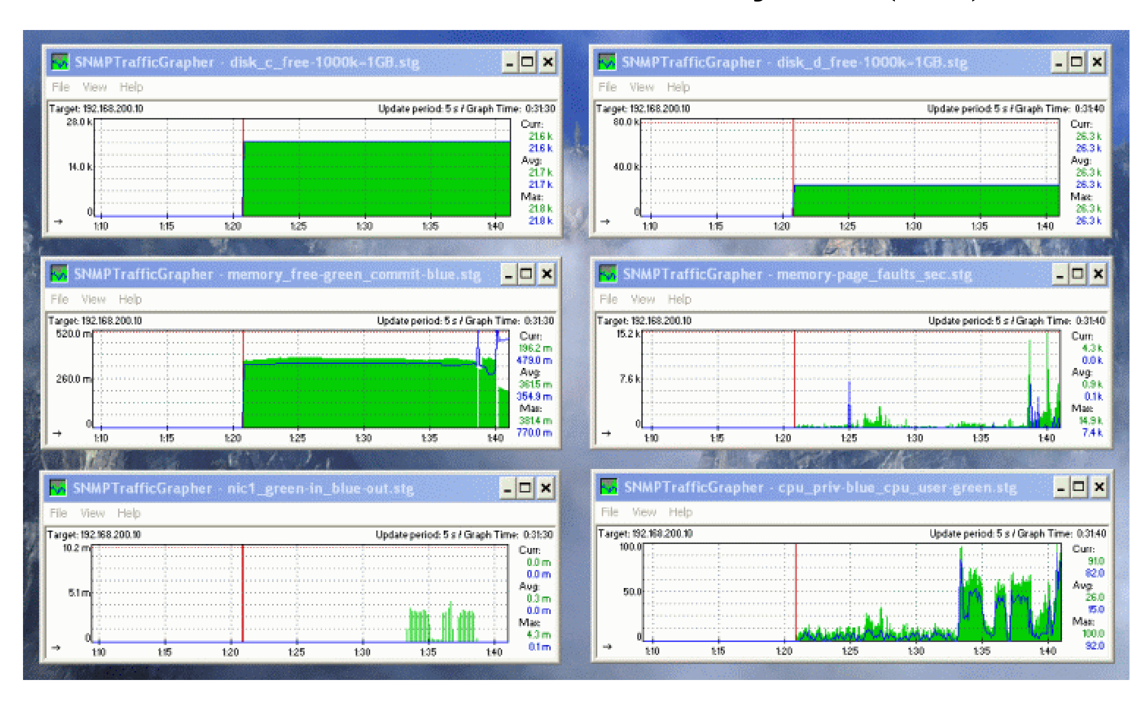
SNMP : هو أحد بروتوكولات الشبكة و هو عامة و يعمل على جميع الاجهزة و وظيفته ادارة الشبكة حيث من خلال هذا البروتوكول نستطيع مراقبة الشبكة بشكل جيد ، و يبداء هذا البروتوكول يمر بثلاث وظائف .

1- SNMP Manager , 2- SNMP Agent , 3- Management Info Base

SNMP Manager : هذا يكون الجهاز الذي يعمل عليه بروتوكول الـ **SNTP**.

SNMP Agent : هذا الاسم الذي يقول عليها على جميع الاجهزة الموجودة في الشبكة و التي سيتم مراقبتها من خلال بروتوكول الـ **SNTP**.

Management Info Base : هذه تعني و ترمز الى قاعدة البيانات التي تكون موجودة في داخل بروتوكول الـ **SNTP** و كل المعلومات المخزنة يتم اضافة عنوان له و يطلق على هذا العنوان **Object ID (OID)**.



- يوجد أكثر من اصدار لبروتوكول الـ **SNMP** :

1- SNMPv1 , 2- SNMPv2c , 3-SNMPv2u , 4-SNMPv3

- عملية و أوامر بروتوكول الـ SNMP :

1- GET , 2- Respinse , 3- Get Next , 4- Set , 5- Traps , 6- Inform

GET : هذ الامر يقوم بعملية الارسال من الـ **SNMP Manager** الى **SNMP Agent** ليقوم بطلب معين من المعلومات .

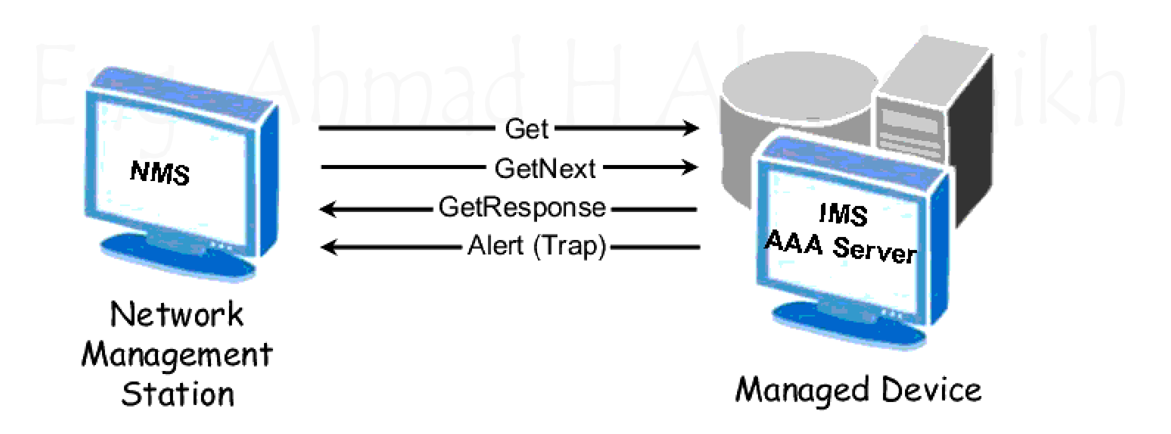
Respinse : هذه عملية الرد على الطلب و اعطاء المعلومات المطلوبة بشكل كامل .

Get Next : هذا الامر لطلب عملية ارسال معلومات اضافية عن الطلب المراد .

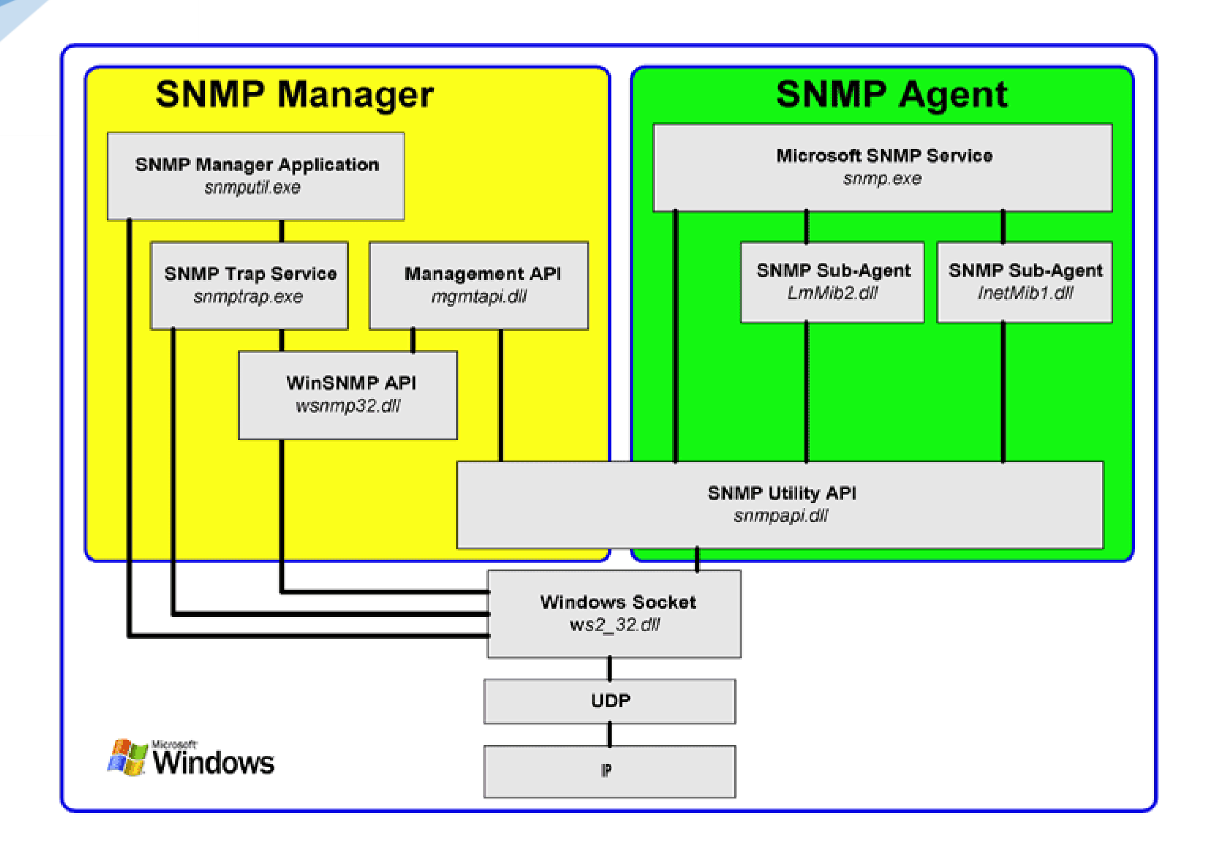
Set : هذا الامر يقوم بعملية ارسال من الـ **SNMP Manager** و يحتوي على إعدادات مثل عنوان الـ **IP** و الكثير من المعلومات الآخر .

Traps : هذا الامر لجمع معلومات مهم جداً جداً حيث انه يقوم بعملية ارسال رسالة لمدير الشبكة .

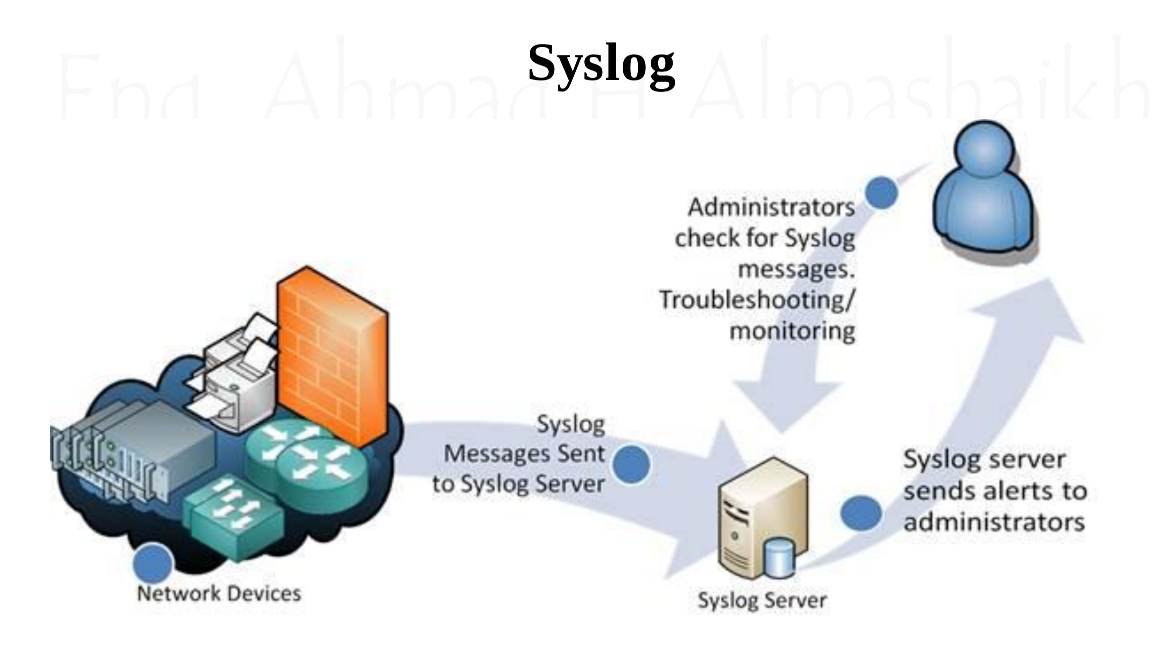
Inform : هذا الامر يقوم بتاكيد على استلام البيانات و المعلومات بشكل صحيح .



- بروتوكول الـ **SNMP** يعمل في داخل بروتوكول الـ **UDP** و ياخذ رقم البروت **161** , **162** .



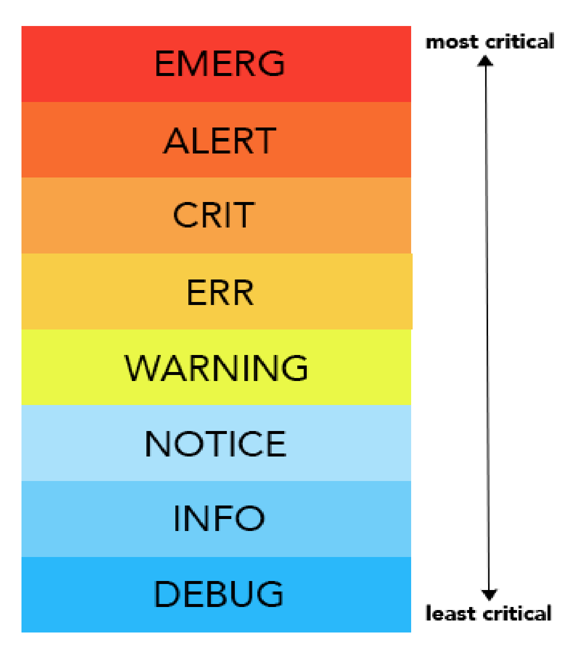
Syslog



Syslog : هو عبارة عن تطبيق أو برنامج وظيفته مراقبة الاجهزة التي تعمل في داخل الشبكة ، مثل الحواسيب و السيرفرات و المستخدمين و الطابعات و السيويتشات و الراوترات و الكثير من الاجهزة الآخر وذلك على عدة مستويات من المراقبة على اخذ الاجراء المناسب **Action** .

- يتم نقل البيانات عن طريق بروتوكول الـ **UDP** و ياخذ رقم **Port 514** .
- البرامج التي تقوم بتشغيل ملف الـ **Syslog** (**Kiwi Syslog** , **Spluck**).

Syslog Levels مستويات الملفات و هي عبارة عن ثمانية رسال تبداء من الصفر حتى ثمانية سنفهم كل رسال ماااذا تفعل .



1- **Emergencies** رسالة الطورئ
2- **Alerts** رسالة التحذير من حدوث خطاء
3- **Critical** رسالة الاحداث التي تكون اقل خطوره من حدوث الخطاء
4- **Error** رسالة الاخطاء و تعني انه يوجد خطاء قد حدث
5- **Warning** رسالة التحذيرات عند حدوث شيء غريب في و غير معروف النظام
6- **Notifications** رسالة الملاحظة مثل عند دخول مستخدمين
7- **Informational** رسالة كاملة عن المعلومات الخاصة في الجهاز
8- **Debugging** رسالة حدوث مباشر

Switch Ways With Frames

طريقة التعامل مع اطارات البيانات الخاصة في السويتش

Store-and-Forward



Cut-Through



A store-and-forward switch receives the entire frame, and computes the CRC. If the CRC is valid, the switch looks up the destination address, which determines the outgoing interface. The frame is then forwarded out the correct port.

A cut-through switch forwards the frame before it is entirely received. At a minimum, the destination address of the frame must be read before the frame can be forwarded.

1- Cut-Through

هذه حالة السويتش عند وصول الفريم الى السويتش حيث يقوم بنظر الى عنوان المرسل اليه و يقوم بعملية ارسال الفريم الى الجهاز المطلوب ، ولكن عيب هذه النوع انه لا يتاكد من استلام البيانات و صحة وصولها .

2- Store and Forward

هذه الحالة تعن أن يقوم السويتش بتاكد من كل فريم تصل اليه و صحة هذه الفريم و يقوم ايضاً بتخزين نسخة منه ، لتكون بشكل احتياطي في حال الحاجة اليها .

3- Fragment-Free

هذه الحالة هي عبارة عن وسيل تربط ما بين الحالات السابقة حيث يتم التاكد من اول قسم و هو مكون من **64** بت و بعده يرسل باقي الفريم .

Router Ways With Packets

طريقة التعامل مع حزم البيانات الخاصة بجهاز الراوتر أو الموجه

1- Process Switching

هذه العملية تتم عندما يستلم الراوتر البكت و هي حزمة البيانات المرسله للراوتر حيثو انه يقوم بنظر على جدول التوجيه ، و بعده سيتم تحديد اتجاه البكت للمسار الذي يجب أن ترسل منه .

2- Fast Switching

هذه العملية وظيفتها أن يقوم الراوتر بعمل نفس الوظيفة الاولى بحيث يقوم بعملية البحث في جداول التوجيه ، ولكن عندما ا يسلتم بكت اخرى جديد ، بشكل مباشر سيتم اضافة المعلومات الجديد على المعلومات القديمة .

Web Server
IP-adress: 2.17.169.198
Subnet Mask: 255.255.255.0
Gateway: 2.17.169.1

IP address: 2.17.169.198
MAC address: 01:53:aa:f9:d2:6c

Source IP: 195.15.16.11
Destination IP: 2.17.169.198
Source MAC: 35:a0:b1:00:57:c2
Destination MAC: 01:53:aa:f9:d2:6c

IP address: 2.17.169.1
MAC address: 35:a0:b1:00:57:c2

Router

IP address: 203.19.3.58
MAC address: 35:a0:b1:72:01:19

Source IP: 195.15.16.11
Destination IP: 2.17.169.198
Source MAC: 28:18:78:5a:f5:96
Destination MAC: 35:a0:b1:72:01:19

IP address: 203.19.3.57
MAC address: 28:18:78:5a:f5:96

Router

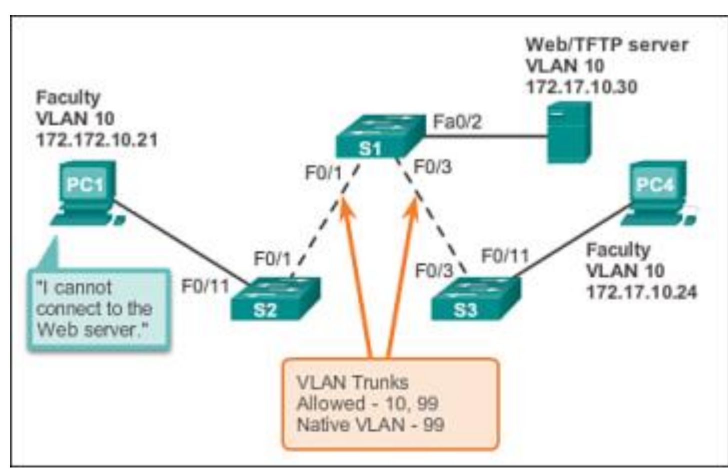
IP address: 195.15.16.1
MAC address: 28:18:78:5a:f4:c7

Source IP: 195.15.16.11
Destination IP: 2.17.169.198
Source MAC: 00:1f:19:ba:20:39
Destination MAC: 28:18:78:5a:f4:c7

IP address: 195.15.16.11
MAC address: 00:1f:19:ba:20:39

Computer
IP address: 195.15.16.11
Subnet Mask: 255.255.255.0
Gateway: 195.15.16.1

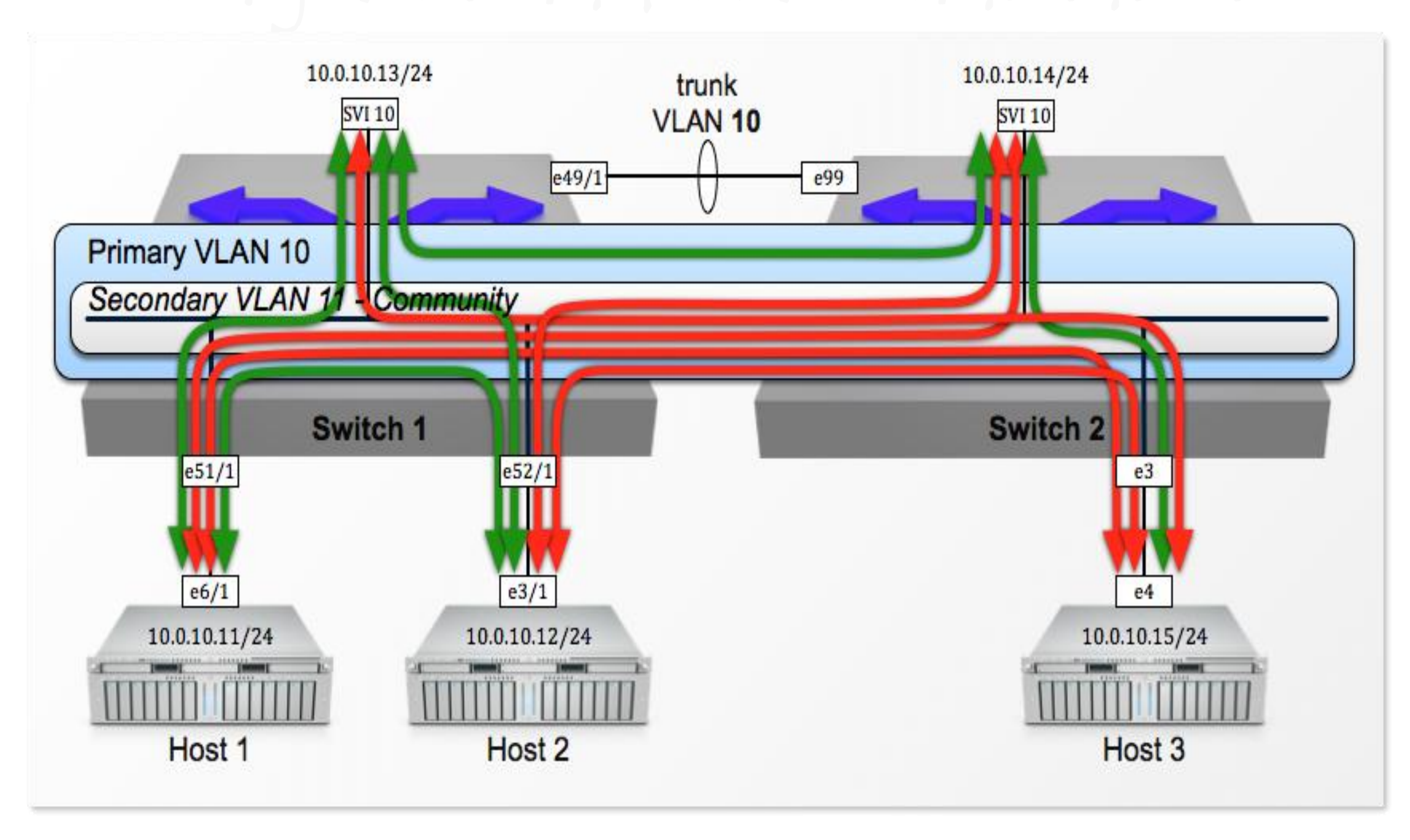
Vlans Allowed in Trunked Interface



Vlans Allowed : هذه العملية من أهم العملية في عالم الشبكة و خصوصي في شبكات الـ **Vlan** مهم جداً جداً في اتجاه الامن ، هذه العملية تقوم بعمل تحديد شبكات **Vlan** معينه على بروت الـ **Trunk Interface** حيث نقوم فقط بمنع نقل هذه الشبكات الى سويتش اخرى تم توصيله في منفذ **Trunk Interface** ، مثل لو يوجد لدينا اربعة شبكات **Vlan** و نريد فقط أن تنتقل شبكتين سنقوم بتحديد الشبكتين الآخر على عدم ارساله الى السويتش الآخر .

Switch (config) # **interface fastethernet 0/1**

Switch (config-if) # **switchport trunk allowed vlan 1-2**



Partial VLANs on inter-switch trunk - No primary VLAN 10 on the trunk

Software - Defined Networking (SDN)



هي منهج أو اسلوب جديد في إدارة شبكات الحاسوب حيث يستطيع مسؤول الشبكة إدارة الشبكة بطريقة مجردة بعيدا عن معرفة تفاصيل الشبكة في الطبقات السفلى و هي الطبقة السابعة بشكل عام ، و تتكون الشبكات المعرفة بالبرمجيات من مستويين : مستوى التحكم **The control plane** وهو عبارة عن الوحدة المركزية والمسؤولة عن اختيار المسار لعملية عبور البيانات في الشبكة بعد الاخذ بالاعتبار لعنوان المستلم وضمان تسليمها لواحدة من عدة وحدات البيانات الموزعة في الشبكة تسمى مستوى البيانات **The Data plane** والتي بدورها تتواصل مع المستخدم النهائي .

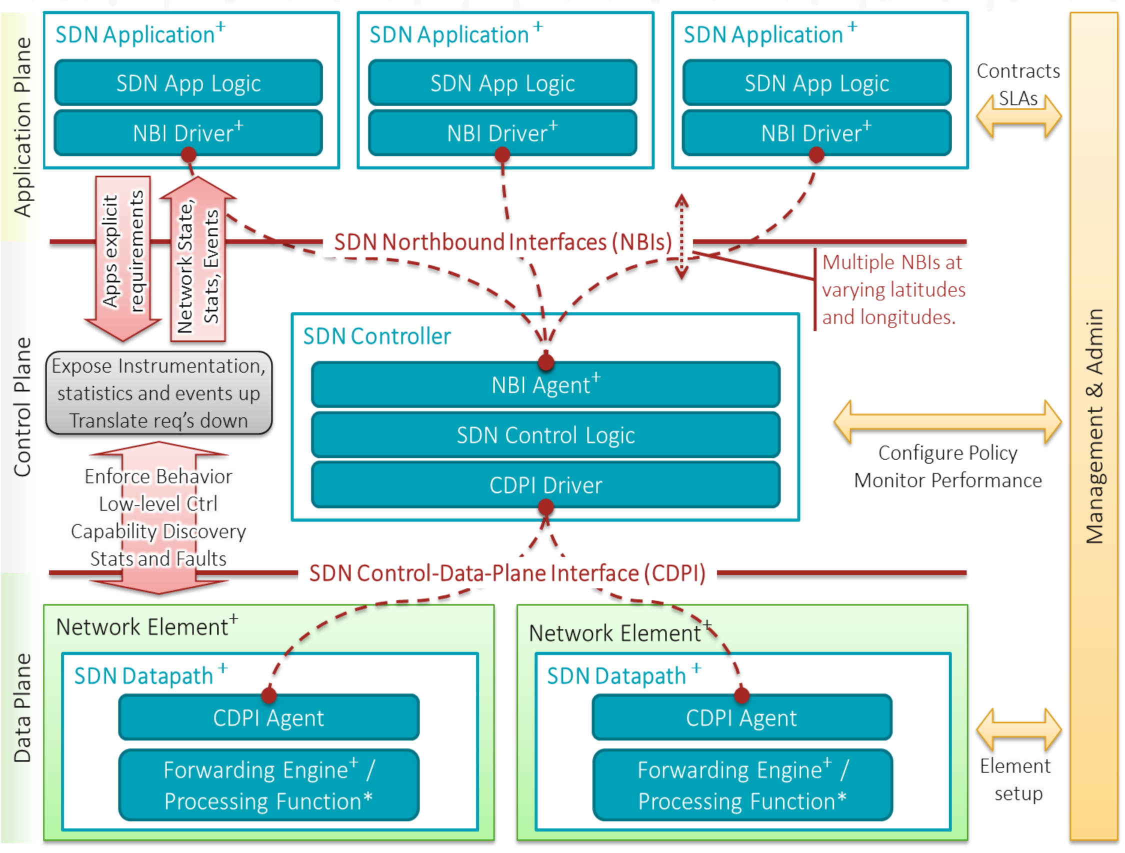
غالباً، يستخدم بروتوكول أوبن فلو **OpenFlow** للتنسيق في عميلة الاتصال بين مستوى التحكم **Control plane** و مستوى البيانات **Data planes** .

مفهوم تقنية الـ SDN :

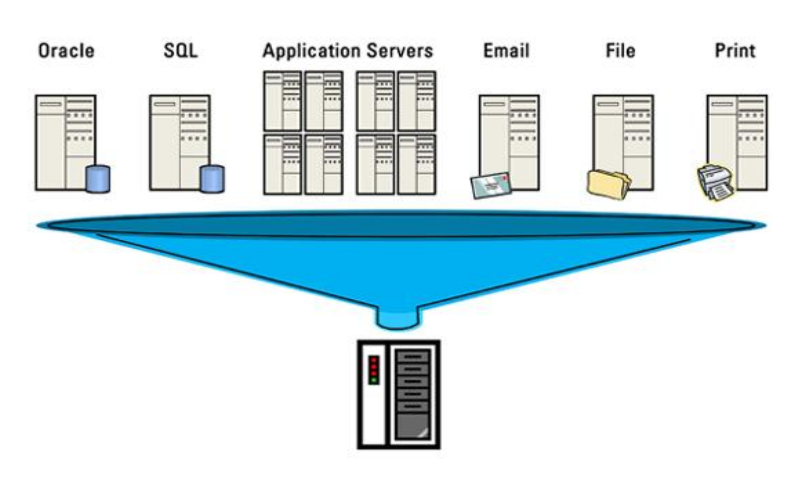
تقنية الـ **SDN** تم اختراعها لتسهيل عملية التحكم في الشبكة بشكل عام من ناحية ادارة و تحكم و في الشبكة ، و العنصر الاساسي الذي تم الاعتماد عليه في بناء تقنية الـ **SDN**هو بروتوكول الـ أوبن فلو و قد تم حل الكثير من المشاكل التي كان مهندس الشبكة يعاني منها و عندما ا تما اختراع هذه التقنية تم حل جميع المشاكل واصبح ادارة الشبكة اسهل بكثير حيث أن مهندس الشبكة يستطيع التحكم في الشبكة من خلال البرامج .

- يوجد بعض المتطلبات قبل أن نتعمق في التعرف على تقنية الـ **SND** يجب أن نكون على معرفة كاملة عن هذه المعلومات مثل ، يجب على مهندس الشبكة أن يكون على معرفة في لغة البرمجة مثل جافا أو بايثون أو روبي ليستطيع عمل برامج للتحكم في الشبكة و يجب أن يكون على معرفة ممتاز في عالم الشبكة ليستطيع عمل هذه البرامج ، وعلى مهندس الشبكة أن يكون بمستوى المحترفين على الاقل ليستطيع العمل في هذا الموضوع ويشترط أن يكون ايضاً على معرفة و دراسة في خاصية و تقنية التطبيقات الوهمية **virtualization** .

- قابلة للبرمجة بشكل مباشر ، و التحكم في الشبكة بشكل مباشر ايضاً .
- يستطيع مهندس الشبكة التحكم في الشبكة بشكل كامل من مكان واحد حيث يقوم بعمل ادارة و تحكم و صيانة من مكان واحد لي انه يوجد شروط في تقنية الـ **SDN** تقوم بتحكم في الشبكة ، حيث يقوم مهندس الشبكة بوضع هذه الشروط .
- تحسين عملية ارسال البيانات في الشبكة حيث من ناحية التوجيه و توزيع الترافيك في الشبكة .
- سهولة صيانة الشبكة و مراقبة الشبكة بشكل اوسع و اسهل ، حيث انه يتواجد وحدة مركزية للتحكم الكامل في الشبكة كلها .
- توفير عدة كبير من أجهزة الشبكة حيث انه نستطيع عمل أجهزة شبكة افتراضية ولكن وهمية وغير موجودة في الواقع .
- سيتواجد شبكات افتراضية برمجية و ستكون اسهل بكثير من أن يكون عدة شبكات موجودة في الواقع الحقيقي ، حيث أنه سيوفر لنا الكثير من الوقت و توفير من ناحية التكلفة و سهولة في الادارة .
- تعمل هذه التقنية مع التقنية التالية مثل **MPLS** , **GMPLS** .
- يستطيع مهندس الشبكة توسيع الشبكة بكل سهولة لي انه بشكل افتراضي و وهمي و هذا يسهل الكثير من العمل على مهندس الشبكة و يكون افضل من أن تكون الشبكة موجودة بشكل حقيقي .
- الحماية ستكون من أعلى مستويات الحماية و الامن ، حيث يستطيع مهندس الشبكة عمل تطبيق أمني موحد و دقيق لكل الشبكة و التحكم فيه ايضاً من مكان واحد .



البيئة الافتراضية , Virtualization



تقنية البيئة الافتراضية تعد هذه التقنية من أهم التقنية الموجودة في عالم التكنولوجيا و هي تقنية مميزة بشكل كبير جداً، و هي التي تمكن المستخدمين من تشغيل أكثر من نظام تشغيل على جهاز الحاسوب الواحد في نفس الوقت الذي يعمل فيها المستخدم حيث يستطيع تشغيل أكثر من نظام مثل الويندوز و الينكس و الماك على نفس الجهاز و في نفس الوقت ، و تعتمد هذه التقنية على موصفات جهاز الحاسوب حيث تحتاج قطع هاردوير ذات الموصفات العالية لتستطيع تشغيل أكثر من نظام تشغيل في نفس الوقت ، ويجب أن نعرف ايضاً انه يوجد أكثر من شركة تقوم بعمل هذه البيئة مثل مايكرسوفوت و **Vm** و لينكس و **Citrix** وكل من هذه الشركات له مميزاتها .

قبل أن نبداء في التعمق بشكل عام في موضوع البيئة الافتراضية يجب أن نعلم أن شركة سيسكو ايضاً بدائة تعمل بهذه التقينة ولكن بشكل اخرى مثل عمل جهاز رواتر افتراضي و جهاز سويتش افتراضي و شبكة افتراضية ايضاً ، ولكن ساقوم بشرح تقنية البيئة الافتراضية بشكل عام لنتعرف عليها و بعدها تستطيع البحث بنفسك عن كيف شركة سيسكو تعمل بهذه التقنية في أجهزة سيكسو .

أنواع البيئة الافتراضية :

يوجد ثلاثة أنواع للبيئة الافتراضية ساقوم بذكرها و شرحها :

Paravirtualization , Binary Translation , Emulation

المحاكاة Emulation :

تعتبر المحاكاة **Emulation** من أكثر النماذج الشائعة لتطبيقات البيئة الافتراضية وتطبق على نطاق واسع في مجال الألعاب ، تمكّن التقنية المستخدم على سبيل المثال من تشغيل نظام ألعاب **Super Nintendo** بنظام التشغيل ويندوز إكس بي مثلا مع بلاي ستيشن **Playstation** وأتاري **Atari 2600** بأنظمة مختلفة وبنفس الوقت ويلقى هذا النوع من البيئة الافتراضية من ثغرة تتمثل بتكاليف المعالج الباهظة عند محاكاة وتقليد الأنظمة و الأجزاء الصلبة وما يرافقها من ضياع للوقت.

Paravirtualization : يلقى نموذج البيئة الافتراضية **PV** إقبالا متزايدا من المستخدمين والشركات على حد سواء كشركة صن **Sun** التي أعلنت مؤخرا تبنيها هذا النموذج. ويجعل أنظمة التشغيل المستضافة تتعرف على أنها بحالة افتراضية ويوفر توافقا بينها. ويوافق نموذج **PV** أنظمة التشغيل مفتوحة المصادر مثل لينكس و **xBSD** ولا يناسب ويندوز.

Paravirtualization

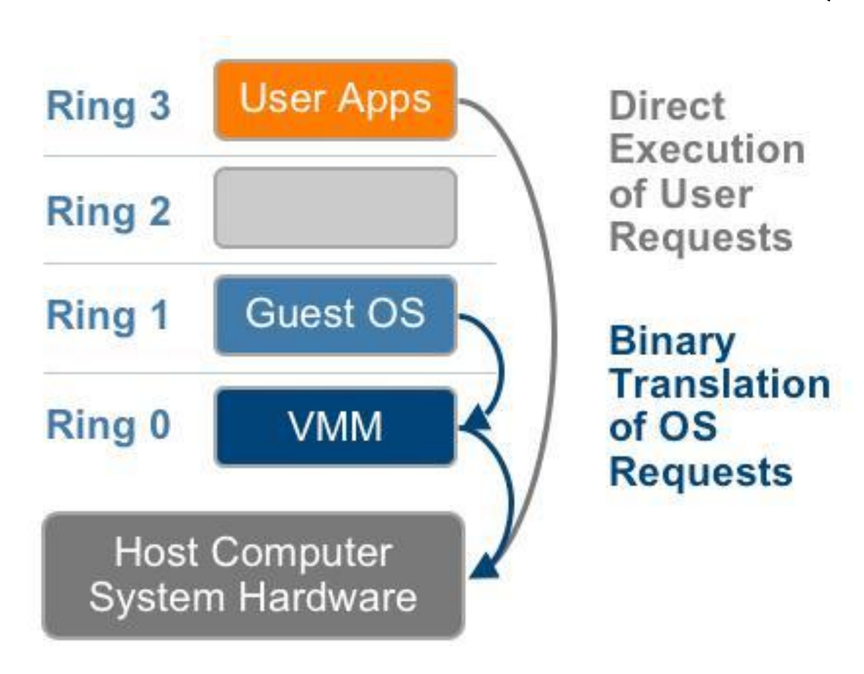
Apps	Apps	Apps	Apps	Apps	Apps
Guest OS	Guest OS	Guest OS	Guest OS	Guest OS	Guest OS
Modification	Modification	Modification	Modification	Modification	Modification

Hypervisor

Host OS

HARDWARE

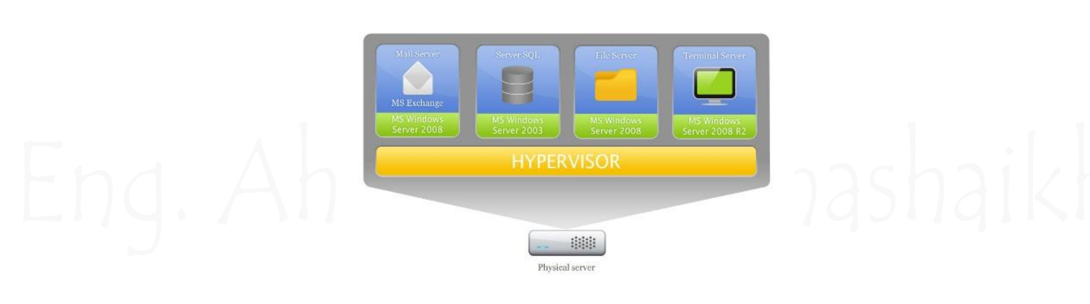
Binary Translation : يعمل النوع **BT** على تعديل الأوامر التي ينفذها الخادم و المضيف في حال وجود خلل أو مشاكل، فعندما ا يحاول نظام التشغيل تنفيذ أمر ما **XYZ** والذي قد يسبب مشاكل للخادم، يقوم **BT** بتعديل الأمر لآخر آمن. ولا يخلو هذا النوع من عيوب تتلخص بالزمن الذي سيستغرقه المعالج في التعرف على الأوامر المغلوطة واستبدالها بأخرى صحيحة.



نظام الإدارة الافتراضي :

تشير توقعات كثيرة إلى انتشار البيئة الافتراضية على نطاق واسع في المستقبل القريب مع انخفاض ملحوظ في تكاليفها، وقد يكون قطاع الخواديم من أقل القطاعات حماسا لثورة التقنية الافتراضية في حين سيشهد قطاع مستخدمي الشركات الكبيرة تغيرات حاسمة أهمها نظام الإدارة الافتراضي للأجهزة والذي يشكل جزءا لا يتجزأ من رزمة برامج الإدارة التي يمكن تنزيلها على الأجهزة وإجراء التعديلات عليها. يمكن نظام الإدارة الافتراضي المستخدم من تتبع البرامج غير المشروعة المستخدمة في الحاسوب مثلا وإيقافها أو تحميل وإلغاء البرامج المخزنة على القرص الصلب ، وإن حاول أحد المستخدمين العبث بملفات نظام التشغيل مثلا يمكنك إلغاء النظام فورا واستبداله بآخر وبسرعة كبيرة، وكذلك الحال مع الفيروسات والبرامج التخريبية التجسسية. وستزوّد إنتل نظام **Virtual Machine Manager** **VMM** كميزة معيارية في شرائحها مع تقنية **VT** في معالجات بنتيوم **4** التي أو في معالجات ثنائية تلقب حاليا بـ "سميثفيلد" التي ستطرحها الشركة في النصف الثاني من هذا العام.

كيفية عمل البيئة الافتراضية :



يتطلب إنشاء خادم افتراضي مستضاف ذاكرة بسعة ٤ كيلوبايت واستخدام الأمر **VMPTLRD** الذي يحول هذه الذاكرة إلى مكان تتوضع فيه جميع البتات عنما يكون نظام التشغيل في حالة سبات وتبقى هذه المنطقة طالما بقي نظام تشغيل نظام التشغيل بحالة جيدة ولا يواجه أية مشاكل. وللتحكم بالجهاز الافتراضي يمكن استخدام أحد الأمرين **VMLaunch** و **VMResume** .

- يعمل الأمر **VMResume** على تعريف حالة المعالج من منطقة الذاكرة ليتحكم بعدها بنظام تشغيل الخادوم المستضاف.
- يقوم الأمر **VMLaunch** بنفس المهام إلا أنه ينشأ نموذجا للتحكم بالجهاز الافتراضي **Virtual Machine Control Structure** حيث يتم تحديد المهام المطلوبة والممنوعة وتكون النتيجة سرعة في الأداء ونظاما متكاملا.

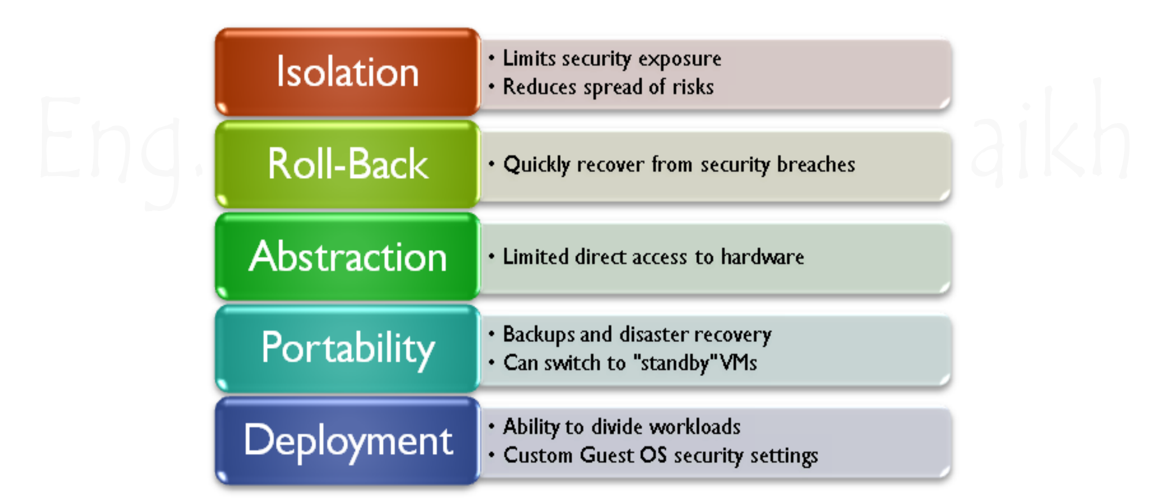
قد يتبادر إلى ذهن القارئ كيف يمكن تعطيل نظام التشغيل هذا والانتقال للعمل بنظام آخر، يلعب عدد من الأنماط النقطية **Bitmaps** في بيئة التحكم بالآلة الافتراضية **VMCS** دورا مهما هنا. تتكون الأنماط من **32** بت يمثل كل واحد منها مهمة معينة وإذا حصل خلل في ذلك البت يختار المعالج التوقف عن العملية ويحوّل الأمر **VMResume** إلى الخادم المستضاف الآخر ليعود النظام إلى حالته الطبيعية.

خيارات واسعة من البيئة الافتراضية :

تعد البيئة الافتراضية ذات طبيعة ديناميكية مرنة تتماشى مع التطور التقني الذي يشهده قطاع تقنية المعلومات، وتتنوع خيارات هذه البيئة فمن الممكن مثلا إنشاء بيئة افتراضية جزئية فبدلا من جعل كامل النظام بوضع افتراضي يمكن اختيار أجزاء من هذا النظام وتحويلها للحالة الافتراضية ليعمل كل برنامج على جهاز افتراضي بشكل مستقل عن بقية البرامج ولتوفر على المستخدم تكاليف شراء عدد من الحواسيب يساوي عدد المستخدمين الفعليين.

الحلول الأمنية للبيئة الافتراضية :

توفر البيئة الافتراضية قائمة طويلة من مزايا الحماية أهمها تفحص البرامج غير المناسبة والتعرف عليها ورفض تنزيلها على الجهاز الافتراضي، فعند تتصفح مواقع شبكات الانترنت مثلا يقوم النظام بجمع معلومات عن عملية التصفح هذه قبل إغلاق الجهاز الافتراضي وسيتعذر على الفيروسات الانتشار عن تشغيل المتصفح في المرات القادمةنظرا لتحميل النظام لملفات كوكيز المفيدة.



مستقبل البيئة الافتراضية :

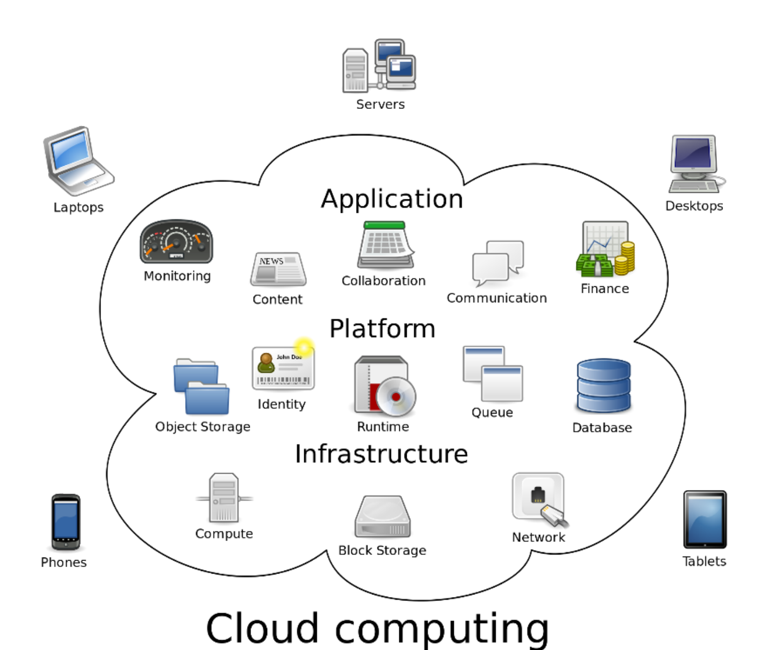
تعد تقنية البيئة الافتراضية من التقنيات المتنامية وسيمضي بعض الوقت على تبني الحواسيب المكتبية لهذه البيئة نظرا لتوقف انتشار هذه التقنية على توفر دعم لها في انظمة التشغيل المختلفة، وعدم ملائمتها للتطبيقات المستخدمة في هذا النوع من الحواسيب، ولكن إنتل حلت هذه المعضلة عن طريق تعاملها مع شركات برامج لتقديم دعم لها في برامجهم دون الاعتماد على دعم انظمة التشغيل .ويتبنى مطورو البرامج و انظمة التشغيل هذه التقنية إضافة إلى الشركات المتخصصة بإنتاج مكونات الحاسوب الصلبة أمثال **IBM**، وقد تعاني البيئة الافتراضية من سلبيات أهمها انخفاض أداء الجهاز الافتراضي وليكن الحاسوب مثلا عند تنزيل أكثر من نظام التشغيل إضافة إلى التكاليف الباهظة، إلا أنه يمكن التغاضي عن جميع هذه السلبيات لحساب المزايا الإيجابية التي تقدمها هذه البيئة.

Cloud Technology



الحوسبة السحابية : هي مصطلح يشير إلى المصادر والأنظمة الحاسوبية المتوافرة تحت الطلب عبر الشبكة والتي تستطيع توفير عدد من الخدمات الحاسوبية المتكاملة دون التقيد بالموارد المحلية بهدف التيسير على المستخدم، وتشمل تلك الموارد مساحة لتخزين البيانات والنسخ الاحتياطي والمزامنة الذاتية، كما تشمل قدرات معالجة برمجية وجدولة للمهام ودفع البريد الإلكتروني والطباعة عن بعد، ويستطيع المستخدم عند اتصاله بالشبكة التحكم في هذه الموارد عن طريق واجهة برمجية بسيطة تُبَسِّطُ وتتجاهل الكثير من التفاصيل والعمليات الداخلية.

و قبل أن نتعمق في شرح هذه التقنية ايضاً يجب علينا أن نكون على معرفة أن شركة سيسكو تعمل بهذه التقنية بشكل واسع و كبير و يوجد بما يسمى كورس كامل مختص في تقنية الـ **Cloud Tech** ، و لكن في هذه الدرس ساقوم بشرح بشكل عام عن هذه التقنية لنتعرف عليها و نكون على معرفة بها ولو بشكل اساسي ولكن اذا تريد التعمق و التعرف اكثر في هذه التقنية تستطيع البحث و المتابعة عن هذه التقنية .



طريقة عمل تقنية الـ Cloud Technology :

عندما ا يصل المستخدم إلى سحابةٍ ما لموقعٍ إلكترونيٍ مناسبٍ، فمن الممكن وقوع العديد من الأمور. فعلى سبيل المثال يمكن استخدام **IP** لإنشاء مكان تواجد ذلك المستخدم الموقع الجغرافي حيث يمكن الاستفادة بعد ذلك من خدمات نظام اسماء النطاقات **DNS** في توجيه المستخدم إلى مجموعةٍ من الخدمات القريبة من المستخدم والمرتبطة به، ومن ثم يمكن الولوج إلى الموقع الإلكتروني بسرعة بواسطة استخدام لغته المحلية الخاصة به. وهنانلاحظ أن المستخدم لا يقوم بالولوج إلى الخادم، إلا أنه يقوم بالولوج بدلاً من ذلك إلى الخدمة التي يقومون باستخدامها من خلال الحصول على هوية جلسة العمل **session id** وأو سجل التتبع الكوكي والذي يتم تخزينه في متصفح الويب الخاص بهم.

فما يشاهده المستخدم على متصفحه غالباً ما يَرِدُ إليه من مجموعةٍ من خواديم شبكة الإنترنت. وتتسم خويدمات شبكة الإنترنت تلك بتشغيل البرامج التي تُشْرِكَ المستخدم مع الواجهات التفاعلية التي يتم استخدامها لجمع الأوامر أو التعليمات من المستخدم نقرات الفأرة، الكتابة والتحرير، عمليات رفع الملفات، حيث يتم تفسير تلك الاوامر بعد ذلك بواسطة خويدمات شبكة الإنترنت أو يتم معالجتها بواسطة خواديم (ملقمات) التطبيقات المختلفة. ثم يلي ذلك تخزين المعلومات على أو استرجاعها من خواديم قواعد البيانات أو حتى خويدمات الملفات، حيث يحدث في النهاية أن يحصل المستخدم على صفحةٍ محدَّثَةٍ. ولنا أن نلاحظ أن البيانات عبر الخويدمات المختلفة تكون متزامنةً حول العالم أجمع بهدف السماح لكافة المستخدمين في مختلف بقاع العالم بالوصول إليها والولوج إلى المعلومات المتوفرة عبرها.

مقارنات ما بين الحوسبة السحابية خصائصها من، ولكن لا يجب أن تتداخل مع:

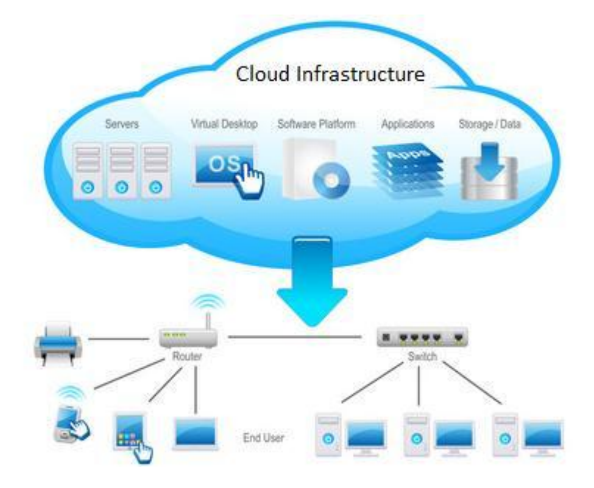
الحواسيب الادارية (**Autonomic Computing**) هي عبارة عن "أنظمة الحاسوب القادرة على ادارة ذاتها .

نموذج المضيف أو الخادم (**Client-server model**) يشير مصطلح حوسبة الزبون الخادم بصورةٍ واسعةٍ إلى تطبيق موزع يقوم بالتمييز بين موفري الخدمة (الملقمات) وطالبي الخدمة العملاء أو الزبائن

الحواسيب الشبكية هي عبارة عن صورة من صور الحواسيب الموزعة و الحواسيب المتوزعة ، حيث يتكون هنا كمبيوتر عملاق أو افتراضي و مجموعة من أجهزة الحاسوب المتشابكة معاً والمتزاوجة بحريةٍ فضفاضةٍ والتي تعمل في تناغمٍ معاً للقيام بمهام ضخمةٍ وكبيرةٍ.

الحواسيب الكبيرة هي عبارة عن أجهزة حاسوبٍ قويةٍ تُستخدم أساساً من قِبَلِ المنظمات العملاقة بهدف القيام بالتطبيقات الحرجة، والتي عادةً ما تكون عبارةٍ عن معالجة للبيانات الضخمة والتي منها على سبيل المثال تعدادات السكان ، الصناعة والاحصائيات الاستهلاكية، تخطيط موارد المؤسسات، و معالجة المعاملات المالية **Transaction processing** .

البنية التحتية Cloud infrastructure :

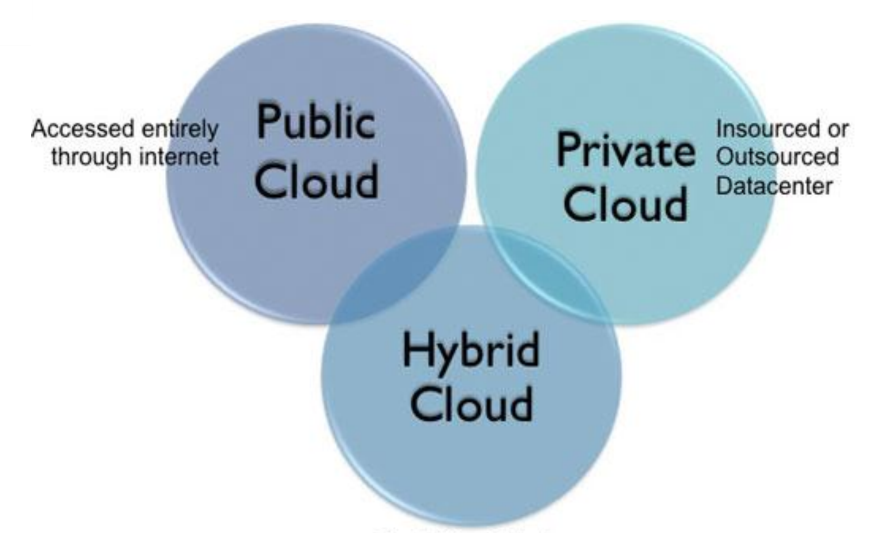


في حين توصل خدمات البنية التحتية للسحابة، والمعروفة كذلك "بالبنية التحتية كخدمة **Infrastructure as a Service** بنية الحواسيب التحيتة غالباً ما تكون بيئة افتراضية متكونة من معددة (**hardware virtualization**) كخدمةٍ حاسوبيةٍ وذلك بدلاً من شراء الملقمات، البرمجيات، أجهزة ومعدات الشبكة أو مساحة مراكز البيانات، حيث يقوم العملاء هنا بشراء تلك المصادر كخدمة الاستعانة بمصادرٍ خارجيةٍ بالكامل. ويحصل ممولوا تلك الخدمة على فواتيرهم غالباً وفقاً لأساس الحوسبة الخدمية وكمية المصادر التي تم استخدامها (ومن ثم التكلفة) ستعكس عادةً مستوى النشاط. وهنا نلاحظ أن خدمات البنية التحتيةللسحابة ظهرت وارتقت من عروض الخادم الافتراضي الخاص غالباً ما تتخذ خدمات البنية التحتية للسحابة صورة مركز بيانات من الدرجة مع العديد من سمات الدرجة الرابعة .

التطبيقات التي تقوم فيها خدمة الـ Cloud :

- التصفح والوصول القائم على الشبكة للبرمجيات الحاسوبية المتوفرة تجارياً بالإضافة إلى إدارتها وضبطها.
- الأنشطة التي يتم التحكم بها وإدارتها من مواقعٍ مركزيةٍ بدلاً من موقع كل عميلٍ على حدةٍ ، والتي تمكن العملاء من الوصول إلى التطبيقات عن بعد عبر شبكة الإنترنت.
- توصيل التطبيقات والتي غالباً ما تكون أقرب إلى نموذج واحد للعديد نموذج أحادي ، بنية متعددة المستأجر من نموذج واحد إلى واحد، متضمنةً خصائص كلٍ من البنية، السعر أو التكلفة ، الشراكة والإدارة.
- تحديث ميزة المركزية، والتي تُجَنِّب الحاجة إلى الباتشات المحملة أو التحديثات.
- تستطيع تخزين ما تردي في الـ **Cloud** حيث لان تفقده مهما حصل لديك في داخل الشركة أو في داخل جهازك .
- تستطيع رفع ملفات مهم ، و برامج و حتى نظام تشغيل كامل تستطيع ايضاً رفعها على الـ **Cloud** .
- و يوجد برامج و انظمة نستطيع أن نقوم بأستاجر هذه البرامج و العمل عليها .

نماذج الحواسيب السحابية Cloud Computing Types :



يوجد أكثر من نوع أو نموذج من تقنية الحواسيب السحابية سنتعرف على الأنواع و نعرف كيفية العمل فيها و نفهم كيف تعمل و ما وظيفة كل نوع من هذه الأنواع .

السحابة العالمة Public Cloud : تصف السحابة العامة أو السحابة الخارجية الحوسبة السحابية من منظورٍ تقليديٍ رئيسيٍ، حيث يتم توفير المصادر وفقاً لأساسٍ الخدمة الذاتية المزاجية عبر شبكة الإنترنت، وذلك من خلال تطبيقات الويب وخدماتها، وذلك من طرفٍ ثالثٍ مزودٍ للخدمة بعيداً عن الموقع والذي يقوم بتحصيل الفواتير والنفقات بناءً على أساس الحوسبة الخدمية.

السحابة المشتركة : من الممكن إنشاء سحابةٍ مشتركةٍ حيث يكون للعديد من المنظمات متطلباً متماثلةٍ وتسعى إلى مشاركة البنية التحتية بهدف تحقيق بعض المصالح والفوائد التي تعود من وراء الحوسبة السحابية. فمع انتشار وتوزيع التكلفة فيما بين مستخدمين أقل من السحابة العامة (ولكن أكثر من مستأجرٍ واحدٍ) ، يصبح ذلك الاختيار أكثر تكلفةٍ ولكنه يُوفر مُسْتَوًى أعلى من الخصوصية، الأمن و أو سياسة الامتثال ومن الأمثلة على السحب المجتمعية المشتركة سحابة جوجل غاف كلود **Gov Cloud**.

السحابة مُرِكَّبَة : من الأصح أن يُطلَق على سحابتين تم ارتباطهما واشتراكهما معاً اسم "سحابةٍ مركبةٍ". حيث تكون بيئة السحابة المركبة المكونة من مزودين خارجيين و أو داخليين متعددين بيئةً نموذجيةً لمعظم المشاريع فمن خلال دمج خدمات سحبٍ مركبةٍ معاً، يستطيع المستخدمون حينئذٍ تسهيل عملية التحول لخدمات السحابة العامة بينما يصبحون قادرون على تجنب القضايا مثل إلزام معيار أمن بيانات صناعة بطاقة الدفع **Payment Card Industry Data Security Standard**.

السحابة المُوَلَّدة (الهجينة) وتوصيل تقنية المعلومات الهجينة : تتمثل المسؤولية الرئيسية لقسم تقانة المعلومات في توصيل الخدمات للأعمال المختلفة. فمع انتشار الحوسبة السحابية (العامة والخاصة كلتيهما) وحقيقة أنه يجب على أقسام التقانة المعلوماتية كذلك توصيل الخدمات عبر السبل التقليدية داخل المنازل، أصبح المصطلح الأكثر تداولاً هو "الحوسبة السحابية الهجينة **hybrid cloud computing** هذا ويُطلق على السحابة الهجينة كذلك التوصيل الهجين وذلك من قِبَل الباعة الرئيسيين في المجال ومنهم **hp**، **ibm**، أوركل (**VMware**)، ، والذين يعرضون التقانة للتغلب على مشكلة تعقد عملية إدارة الأداء، المخاوف الأمنية والخصوصيات والتي تنتج من خلط طرق توصيل خدمات التقانة المعلوماتية. وهنا تستخدم سحابة التخزين المهجنة تركيبيةً من سحب التخزين الخاصة والعامة. وغالباً ما تكون سحب التخزين المهجنة مفيدةً لوظائف الأرشفة وإنشاء النسخ الاحتياطية والدعم، مما يسمح بنسخ البيانات العامة إلى سحابةٍ عامةٍ .

ومن وجهات النظر الآخر حول انتشار تطبيقات الويب في السحابة استخدام مضيف الويب المهجن **Hybrid Web Hosting** ، حيث تكون البنية التحتية للمضيف عبارة عن خليط فيما بين مضيف السحابة والخواديم المخصصة للإدارة ويُعَدُ هذا الجزء الأكثر شيوعاً وانجازاً من عنقود الويب والتي فيها يتم تشغيل بعض العُقَد على عتادٍ فيزيائيٍ حقيقيٍ والبعض الآخر يتم تشغيله على نماذج خوادم السحابة.

السحابة خاصة Private Cloud : مفهوم الشبكة الخاصة هو يندرج تحت أسم خاص بمنعى أن تكون الشبكة خاصة و السحابة خاصة ، مثل ليكون لدينا شركة خاصة في قطاع خاص أو قطاع حكومي و نريد عمل سحابة خاصة في هذا القطع حيث لا أحد يشترك فيه الا القطاع الداخلي فقط و تكون هذه السحابة ملكية خاصة للقطاع على عكس السحابة العامة التي يشترك فيها جميع الناس .

الهندسة السحابية Cloud engineering: تمثل الهندسة السحابية منهجيةً متاخلةً توليفيةً منظمةً نظاميةً نحو تصور، تطوير، عملية وصيانة الحوسبة السحابية، بالإضافة إلى الدراسة والبحث التطبيقي لذلك المُدخل، مثل تطبيق الهندسة إلى السحابة. فهي تُعَدُ نظاماً ناضجاً راقياً لتسهيل تبني، تصور، تطوير، تنمية، معيارية، إنتاجية، تسويق، وضبط الحلول السحابية، مؤديةً بذلك إلى نظاماً إيكولوجياً سحابياً. كما أن الهندسة السحابية معروفة كذلك بأنها هندسة الخدمة السحابية.

التخزين الساحبي cloud storage : يعبر التخزين السحابي عن أحد نماذج تخزين البيانات الحاسوبية عبر الشبكة حيث يتم تخزين البيانات على العديد من المخدمات الافتراضية، والتي عموماً ما يتم استضافتها من قبل طرفٍ ثالثٍ، بدلاً من أن يتم استضافتها على خواديمٍ محددةٍ. وتقوم شركات الاستضافة بتشغيل العديد من المراكز؛ وهؤلاء الذين يطلبون استضافة معلوماتهم يشترون أو يستأجرون سعةً منهم ويستخدمونها لمتطلبات تخزينهم. وهنا يقوم مشغلوا مراكز البيانات ، في الخلفية، بجعل المصادر افتراضية وفقاً لمتطلبات الزبون ويعرضون عليهم العديد من الملقمات الافتراضية ، والتي يستطيع الزبائن أو العملاء إدارتها بأنفسهم. ومن الناحية المادية قد يمتد المصدر أو المورد عبر عدة خوادمٍ.

أمن الحواسيب السحابية Cloud computing security : تمثل قضية الأمن النسبي لخدمات الحوسبة السحابية مسألةً مستمرةً والتي قد تؤجل من العمل بها .حيث تتجسد القضايا المعيقة لتبني الحوسبة السحابية بصورةٍ أساسيةٍ في القلق الذي يساور القطاعين العام والخاص حول الإدارة الخارجية للخدمات القائمة على الأمن. فالسمة المسيطرة على الخدمات القائمة على الحوسبة السحابية، سواءً في القطاعين العام والخاص، أنها تحفز الإدارة الخارجية للخدمات المتوفرة. مما يخلق حافزاً ضخماً فيما بين مزودي خدمات الحوسبة السحابية في خلق أولويةٍ لبناء وصيانة إدارةٍ قويةٍ للخدمات الآمنة.

وقد تم تأسيس العددي من المنظمات بهدف توفير المعايير اللازمة لمستقبلٍ أفضلٍ في مجال تقديم خدمات الحوسبة السحابية. ومن تلك المنظمات على سبيل المثال "تحالف الأمن السحابي (**Cloud Security Alliance**) والتي تعتبر منظمةً غير ربحيةٍ تأسست لتعزيز قضية استخدام أفضل الممارسات لتوفير الضمان الأمني ضمن مجال الحوسبة السحابية.

أمن الحوسبة السحابية :

يمكن تعريفه بأنه مجموعة واسعة من السياسات و التقنيات و الضوابط لحماية البيانات المنتشرة و التطبيقات و البنية التحتية المرتبطة بها و المكونة للحوسبة السحابية , أو بصورة أخرى هي تكامل و إندماج أغلب مجالات أمن المعلومات مثل أمن الشبكات و أمن الأنظمة و أمن التطبيقات و غيرها في مجال جديد يعتمد كل جزء فيه على الجزء الآخر في تناغم تام. تنقسم التحديات الأمنية المتعلقة بالحوسبة السحابية إلى قسمين:

- المصاعب و التحديات الأمنية التي تواجه مزود خدمة الحوسبة السحابية .
- المصاعب و التحديات الأمنية التي تواجه مستخدم خدمة الحوسبة السحابية .

مزود خدمة أمن و حماية الحوسبة السحابية :

يوجد أكثر من خدمة في أمن و حماية الحواسيب السحابية ، والتي يجب أن يكون مهندس الشبكة أو مهندس النظام على معرفة كاملة فيها و معرفة كيف تعمل هذه الخدمات و ساقوم بذكر بعض من هذه الخدمات لنتعرف عليها .

حماية البيانات : حماية البيانات **Data protection** هي أن تكون البيانات محمية و مفصولة و مصانة عن الإختلاط بين المستخدمين و يجب أن يتم التخزين بشكل آمن و أن تكون البيانات قادرة على التحرك بشكل آمن من موقع إلى آخر، كذلك يجب أن تكون البيانات مشفرة وفق أفضل تقنيات التشفير.

الفصل بين الواجبات : يجب الفصل الصحيح و الكامل بين الواجبات و الوضائف (**segregation of duties**) حتى يضمن أن خدمات كالمراقبة و الرصد و التدقيق سواء أكانت من مزود الخدمات أو من المستخدمين أو من طرف ثالث تعاقد معه المزود أو المستخدم و لديه إمتياز عن المستخدم العادي لأداء مهمته، يجب الفصل بينهم و تطبيق نظام متكامل لضمان عدم تسرب البيانات.

إدارة الهوية : توفير إدارة الهوية و التحكم بالدخول للمصادر المعلوماتية و موارد الخدمة، وفقا لإحتياجات المستخدم على أن تقبل هذه الأنظمة التكامل و قابلية الدمج و التطوير مع أنظمة إدارة الهوية (**Identity management**) الخاصة بالمستخدم سواء أكانت تقليدية أو أنظمة مقدمة من مزود آخر للخدمة فيما يعرف بعملية الإتحاد **federation services**.

الأمن المادي أمن الأجهزة و المعدات : مزود الخدمة يجب أن يضمن أن الأجهزة و المعدات آمنة بشكل كاف و لا يمكن الوصول إليها بأي شكل من الأشكال، و مقيدة بنظام دخول متكامل و موثق للرجوع إليه عند الحاجة، و قد يكون جزء من نظام إدارة الهوية في حالة المستخدمين ذوي الإمتيازات الخاصة.

التوافرية : مزود الخدمة يضمن أن المستخدمين سوف يحصلون على توفيرية للخدمات أو بصورة أخرى قابلية الوصول إلى البيانات و الأنظمة و التطبيقات الخاصة بهم بشكل منتظم، و متاح طوال فترة الخدمة دون أي توقف.

أمن التطبيقات و الأنظمة : مزود الخدمة لا بد أن يضمن أمن و سلامة التطبيقات و الأنظمة المقدمة ضمن الخدمة من خلال تنفيذ الإختبارات و تطبيق السياسات و الإجراءات و نظم الحماية متعددة الطبقات.

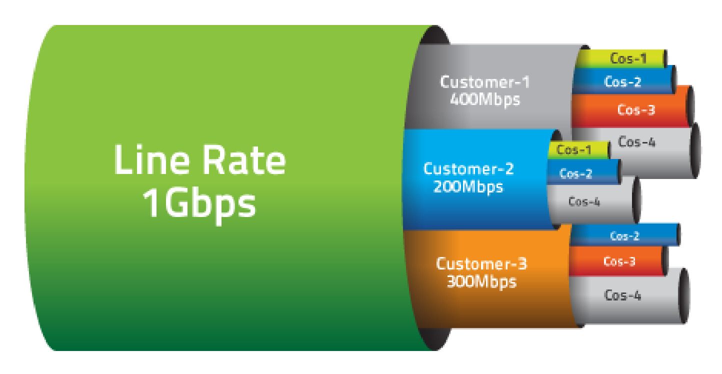
السرية : مزود الخدمة لابد أن يضمن السرية التامة للمتخدم للبيانات بكل أنواعها، و عدم السماح بالوصول لها إلا للأشخاص المخولين من قبل المستخدم.

حقوق مستخدم خدمة الحوسبة السحابية :

حقوق المستخدم و المسؤليات الواقعة عليه في النقاط التالية:

- الحق في الحفاظ على الملكية و إستخدامها و السيطرة على البيانات الخاصة .
- الحق في الحصول على اتفاق مستوى الخدمة يتضمن الإلتزامات التقنية و المادية و الإجراءات العامة .
- الحق في إستقبال الإخطار و حرية الإختيار للتعديلات التي تؤثر في العمليات التجارية للمستخدم .
- الحق في معرفة القيود التقنية أو متطلبات الخدمة مسبقا .
- الحق في معرقة المتطلبات القانونية للدول التي يعمل فيها مقدم الخدمة مقدما .
- الحق في معرقة إجراءات و سياسة عملية الأمن التي يتبناها مزود الخدمة .
- مسؤلية الفهم و الإلتزام بمتطلبات ترخيص البرمجيات و النظم .

Quality of service



جودة الخدمة QOS

يشير مصطلح جودة الخدمة في مجال شبكات الحاسوب وغيرها من شبكات تبديل حزم المعلومات في الاتصالات السلكية واللاسلكية، وهندسة المرور إلى آليات لحفظ السيطرة على الموارد بدلا من تحقيق جودة الخدمات. جودة الخدمة هو القدرة على تقديم أولويةمختلفة لتطبيقات مختلفة، مستخدمين، أو تدفق للبيانات، أو لضمان مستوى معين من الأداء لتدفق البيانات. على سبيل المثال، يمكن ضمان معدل سرعة المعلومات المطلوبة، والتأخر، عدم استقرار الإرسال، احتمالية إسقاط الرسائل أو معدل الخطأ للمعلومات المطلوبة. تعتبر ضمانات جودة الخدمة هامة إذا كانت قدرة الشبكة غير كافية، وخاصة بالنسبة لتدفق التطبيقات ذات الوسائط المتعددة وقت حدوثها مثل الصوت عبر بروتوكولات الإنترنت، والألعاب الإلكترونية والتلفزيون الرقمي التابع لبروتوكولات الإنترنت، لأن هذه غالبا ما تتطلب معدل ثابت لتدفق البيانات، وهي حساسة للتغيير، ومن حيث الشبكات حيث تعتبر القدرة موردا محدودا، على سبيل المثال في بيانات الاتصالات الخلوية. في حالة عدم وجود ازدحام في الشبكة، تعتبر آليات جودة الخدمة غير مطلوبة.

ويمكن أن تتوافق الشبكة أو البروتوكول الذي يدعم جودة الخدمات على عقد المرور مع تطبيق البرمجيات والقدرة الاحتياطية في عقد الشبكة، على سبيل المثال خلال مرحلة إقامة الدورات. وهي يمكن أن تحقق رصدا لمستوى الأداء خلال الدورة، على سبيل المثال معدل البيانات والتأخير، والتحكم ديناميكيا عن طريق جدولة الأولويات في عقد الشبكة. وقد تفرج عن القدرة الاحتياطية خلال مرحلة الهدم.

ولا تستطيع أفضل جهد للشبكة أو الخدمة أن تدعم جودة الخدمة. كبديل لآليات معقدة مراقبة جودة الخدمة هو تقديم نوعية عالية من التواصل عبر شبكة جهد أفضل من الإفراط في توفير القدرة بحيث يكون كافيا لتوقع حركة المرور لتحمل الذروة.

في ميدان الاتصالات الهاتفية ، وجودة الخدمة تم تعريفها الاتحاد الدولي للاتصالات

الموحدة بأنها "مجموعة من متطلبات الجودة على السلوك الجماعي لواحد أو أكثر من الكائنات". نوعية الخدمة تشمل متطلبات على جميع جوانب اتصال، مثل استجابة الخدمة الوقت والخسارة، إشارة إلى نسبة الضوضاء، عبر الحديث، وصدى، المقاطعات، استجابة التردد، ومستويات جهارة الصوت، وهلم جرا. مجموعة فرعية من جودة الخدمة الهاتفية هو

الصف من الخدمة جوس المتطلبات، والتي تضم جوانب اتصال المتصلة سعة وتغطية الشبكة، على سبيل المثال يضمن أقصى قدر من عرقلة الاحتمال واحتمال الانقطاع.

جودة الخدمة يستخدم أحيانا كإجراء والجودة، مع العديد من التعاريف البديلة، بدلا من الإشارة إلى القدرة على موارد الاحتياط. جودة الخدمة أحيانا تشير إلى مستوى جودة الخدمة، أي ضمان جودة الخدمة. ارتفاع جودة الخدمة وكثيرا ما يخلط مع مستوى عال من الأداء أو تحقيق جودة الخدمة، على سبيل المثال ارتفاع معدل بت، وانخفاض الكمون احتمال الخطاء القليل .

وتعريف بديل لجودة الخدمة، تستخدم خاصة في مجال الخدمات طبقة التطبيقات مثل الاتصالات الهاتفية والفيديو، هو توقع عكس نوعية ذاتية من ذوي الخبرة. مصطلحات أخرى مماثلة مع المعنى نوعية التجربة **(QoE)** ذاتية مفهوم الأعمال التجارية، والمستخدم ينظر الأداء، درجة من الارتياح للمستخدم"، "عدد الزبائن السعداء" أو متوسط نقاط الرأي. في هذا السياق، جودة الخدمة هو تأثير تراكمي على ارتياح المشترك لجميع العيوب التي تؤثر في الخدمة.

مشاكل تقنية الـ QOS :

عندما ا استخدم الإنترنت لأول مرة، إلا أنها تفتقر إلى القدرة على توفير جودة الخدمة الضمانات الواجبة لحدود السلطة في مسار الحوسبة. ولذلك فإنه يدير في مستوى جودة الخدمة الافتراضية، أو "أفضل جهد". كانت هناك أربع "نوع من الخدمة" بت وثلاثة "الأسبقية" بت المنصوص عليه في كل رسالة، ولكن تم تجاهلها. هذه البتات في وقت لاحق إعادة تعريفها بأنها **DiffServer** النقاط المدونة (المستوى الثالث)، وإلى حد كبير في تكريم الروابط أطلت على الإنترنت الحديثة.

عندما ا تبحث في علبة محولات شبكات، جودة الخدمة تتأثر بعوامل مختلفة، والتي يمكن تقسيمها إلى العوامل "البشرية" و"التقنية". وتشمل العوامل البشرية : الاستقرار في الخدمة، ومدى توافر الخدمات، والتأخير، ومعلومات المستخدم. وتشمل العوامل الفنية : الموثوقية، والتدرجية، والفعالية، الصيانة، والصف الثاني من الخدمة، وما إلى ذلك .

أشياء كثيرة يمكن أن تحدث لحزم أثناء سفرهم من المنشأ إلى المقصد، مما أدى إلى المشاكل التالية كما يرى من وجهة نظر من المرسل والمتلقي:

الحزم المسقطة :

المسارات قد تفشل في تحقيق اسقاط بعض الحزم إذا كانوا يصلون عندما ا تكتمل المخازن. بعض، لا شيء ، أو كل من الحزم قد انخفضت، وهذا يتوقف على حالة الشبكة، ومن المستحيل تحديد ما سيحدث مسبقا. التطبيق المتلقي قد يطلب اذاعه هذه المعلومات، ربما تسبب حالات التأخير الشديد في النقل العام.

التأخير :

الامر قد يستغرق وقتا طويلا لحزمة لبوغ غايتها، لأنه يحصل على عقد حتى في طوابير طويلة، أو يأخذ طريقا غير مباشر لتفادي الازدحام. في بعض الحالات، يمكن للتأخير المفرط ان يجعل تطبيق مثل هذة الاتصالات عبر بروتوكول الإنترنت أو اللعب عبر الإنترنت غير صالحة للاستعمال.

غضب الحزم :

الحزم من المصدر ستصل إلى الوجهة مع تأخيرات مختلفة. وهناك حزمة تأخير تختلف مع موقفها في قوائم الانتظار من الموجهات على طول الطريق بين المصدر والمقصد، وهذا الموقف يمكن أن تختلف اختلافا لا يمكن التنبؤ به. هذا التفاوت في تأخير كما هو معروف غضب على محمل الجد، ويمكن أن يؤثر على جودة الصوت أو الفيديو.

نهاية طلب إيصال :

عندما ا مجموعة من الحزم ذات الصلة يتم توجيهها من خلال شبكة الإنترنت، حزم مختلفة تتخذ مسارات مختلفة، كل منها تؤدى إلى تأخير مختلفة. والنتيجة هي أن وصول الحزم في ترتيب مختلف عما كانت عليه إرسالها. هذه المشكلة يتطلب البروتوكولات الإضافيةالخاصة المسؤولة عن ترتيب الخروج من الحزم من أجل إقامة دولة المتزامن بمجرد أن تصل إلى وجهتها. هذا مهم بشكل خاص لنقل الصوت والفيديو وتيارات حيث ان الجودة بشكل كبير تتأثر كل من الكمون وعدم وجود **isochronicity** .

الخطأ :

الحزم في بعض الأحيان هي في غير محلها، أو مجتمعة، أو تعرض للتلف، حينما تكون في الطريق. وعندما ا يكتشف المتلقي هذا يطلب من المرسل أن يعيد نفسه.

التطبيقات التي تتطلب جودة الخدمة :

جودة الخدمة قد تكون مطلوبة لأنواع معينة من حركة مرور الشبكة، على سبيل المثال:

الوسائط المتعددة قد تتطلب مضمونة الإنتاجية لضمان حد أدنى من الجودة والمحافظة عليها.

عروض البث التلفزيوني عبر الانترنت كخدمة من مزود الخدمة .

التهاتف عبر بروتوكول الإنترنت أو الصوت عبر بروتوكول الإنترنتقد تتطلب حدودا صارمة من التأخير.

تحادث الفيديو مؤسسة التدريب المهني يتطلب غضب منخفضة والكمون.

إشارة إنذار على سبيل المثال، جهاز الإنذار ضد السرقة .

وصلة مخصصة مضاهاة يتطلب سرعة نقل مضمون ويفرض قيودا على أقصى قدر من التأخير والغضب.

لسلامة التطبيق الحرج ، مثل الجراحة عن بعد قد تتطلب مستوى يضمن التوافر وهذا هو أيضا دعا لجودة الخدمات الثابتة.

مسؤول النظام قد يرغب في تحديد أولويات المتغير، وعادة ما تكون صغيرة، وكميات من حركة لضمان الدورة حتى تستجيب بشكل كبير على مدى ارتباط لادن.

ألالعاب على الإنترنت، مثل المحاكاة يسير بخطى سريعة في الوقت الحقيقي مع لاعبين عدة. عدم جودة الخدمة قد تنتج 'فجوة.'

إيثرنت البروتوكولات الصناعية مثل إيثرنت / الملكية الفكرية التي تستخدم لمراقبة الوقت الحقيقي للآلات .

هذه الأنواع من الخدمة تسمى غير مرن، بمعنى أنها تتطلب مستوى معينا الحد الأدنى من عرض النطاق الترددي والكمون والحد الأقصى لمهمة معينة.

على النقيض من ذلك، يمكن للتطبيقات المرنة الاستفادة من عرض النطاق الترددي إلا القليل أو الكثير متاح. ملف نقل معظم التطبيقات التي تعتمد على برنامج التعاون الفني عموما مرنة.

آليات جودة الخدمة :

كبديل لآليات معقدة مراقبة جودة الخدمة هو تقديم نوعية عالية من التواصل بسخاء على شبكة التزويد بحيث يستند إلى القدرة على تقديرات الحركة لحمل الذروة. هذا النهج بسيط واقتصادي للشبكات مع الأحمال يمكن التنبؤ بها. والأداء مطابق للعديد من التطبيقات. يمكن أن تشمل التطبيقات التي يمكن أن تطالب بالتعويض عن الاختلافات في عرض النطاق الترددي وتأخير كبير مع تلقي المخازن المؤقتة، والتي غالبا ما أمكن على سبيل المثال في الفيديو.

الخدمات التجارية بتكلفة غالبا ما تكون تنافسية مع خدمات الهاتف التقليدية من حيث جودة المكالمة على الرغم من جودة الخدمة الآليات عادة لا تكون قيد الاستعمال على اتصال المستخدم لبلده، وموفر خدمة الإنترنت والاتصال عبر بروتوكول الإنترنت لمقدمي خدمات الإنترنت المختلفة. تحت شروط تحميل عالية، ومع ذلك، تدهور نوعية الصوت عبر بروتوكول الإنترنت إلى الهاتف الخليوي الجودة أو ما هو أسوأ. الرياضيات للحزم المرور تشير إلى أن الشبكة مع جودة الخدمة يمكن التعامل مع أربعة أضعاف العديد من المكالمات الهاتفية مع متطلبات غضب مشددة حيث ان جودة الخدمة واحدة مندون بحاجة لمصدر قرر يوكسل وآخرون ان **60 ٪** من القدرات الإضافية المطلوبة من خلال محاكاة الحركة الملكية الفكرية في ظل افتراضات متحفظة

مقدار المبالغة في تقديم الروابط الداخلية المطلوبة لتحل محل جودة الخدمة يعتمد على عدد من المستخدمين ومطالبهم حركة المرور. كما أن الإنترنت يخدم الآن ما يقرب من مليار من المستخدمين، هناك احتمال ضئيل أن الإفراط في التقديم يمكن أن تلغي الحاجة إلى جودة الخدمة بتكلفة عندما ا يصبح أكثرشيوعا.

الشبكة لاسلكية Wireless LAN



الشبكات اللاسلكية : هي أي نوع من الشبكات الحاسوبية التي تعمل على نقل المعلومات بين العقد من دون استخدام الأسلاك التوصيلات إن هذا النوع من الشبكات ينفّذ عادةً مع نظم نقل معلومات بالتحكم عن بُعد من خلال استخدام أمواج كهرومغناطيسية كالأمواج الراديوية كحامل لإشارة المعلومات. وهذا التنفيذ يتم عادةً في الطبقة الفيزيائية من الشبك.

الحاجة إلى الشبكات اللاسلكية Networks Wireless :

حيث نجح علماء الحاسوب في الآونة الأخيرة إلى استخدام ما يسمى بالشبكات المحلية، والتي يرمز لها **LAN** اختصاراً لكلمة (**Local Area Network**) وأن الهدف الأساسي من ذلك تحقيق الفائدة القصوى المرجوة من الموارد التي تتيحها الأجهزة على الشبكة وبالفعل فقد وفرت هذه الشبكات العديد من الخدمات لمستخدميها حيث مكنتهم من التواصل مع بعضهم البعض عن طريق البريد الإلكتروني والاستفادة من البرامج والتطبيقات بالإضافة إلى إمكانية الولوج إلى قواعد بيانات مشتركة لكن هذا لميمنع من ظهور بعض العوائق والتي بدأت تحد من اتساع استخدام هذه الشبكات يمكن أن نحدد أهم هذه العوائق بما يلي:

الحاجة إلى وصلة فيزيائية حيث يتوجب على الجهاز الاتصال إلى منفذ ثابت مما جعل عدد العقد ضمن الشبكة يميل إلى الثبات، إضافة إلى تقييد المستخدم في مكان معين دون إمكانية

إضافة إلى الانتشار الواسع للحواسب يمكن القول بأن الميزات التي قدمتها ال **WLAN** للأجهزة المحمولة والمفكرات الإلكترونية قد أدت إلى زيادة الطلب على هذه التقنية الجديدة والتي ستلعب دوراً هاماً في حياتنا الإلكترونية في المستقبل القريب حيث يتوجه العالم في العصر الحديث إلى استبدال النظام السلكي الذي تم الاعتماد عليه في العقود الماضية والانتقال إلى عصر جديد من الأجهزة اللاسلكية

ملاحظة: تجدر الإشارة إلى الاختلاف بين ال **Wide Area Network WAN** و **Wireless LAN WLAN** والتي ترسل المعلومات الرقمية إلى مسافات طويلة باستخدام الأنظمة الخلوية بمعدل نقل بيانات منخفض إضافة حاجتها إلى بنية تحتية ذات تكلفة عالية. نقله لأن هذا الأمر يتطلب قطع الاتصال مع الشبكة وإعادة الاتصال من موقع آخر

أما إذا أردنا إضافة عقدة جديدة إلى الشبكة فهذا يعني المزيد من التوصيلات السلكية

والمزيد من المساحة وهذا ما يؤدي بدوره إلى زيادة التكلفة. إن هذه العوامل قد أدت إلى صعوبة في إنشاء هذه الشبكات وارتفاع سعرها مما دعا إلى ضرورة تعديلها بحيث تتلاءم مع متطلبات العصر ،بناءً عليه بدأ التوجه إلى استخدام الشبكات اللاسلكية **Wireless LAN** والتي قدمت الحلول للمشاكل التي عانت منها الشبكات السلكية، حيث أعطت مرونة كبيرة في عملية إضافة عقدة جديدة إلى الشبكة دون الحاجة إلى المزيد من التوصيلات السلكية، والأهم هو إمكانية التنقل بحرية مع الجهاز المحمول ضمن مجال الشبكة ،هذا مع الأخذ بعين الاعتبار الكلفة المنخفضة لهذه الشبكات.

تعريف الشبكات اللاسلكية

الشبكات المحلية اللاسلكية (**WLAN**) أصبح الآن بإمكان الشخص التنقل في اي مكان يريده وحتى بالأماكن العامة وهو حاملا جهاز الحاوسب المحمول أو ال(لاب توب) وبدون اي أسلاك يستطيع ان يرسل أو يتلقى اي بريد إلكتروني والتصفح في الإنترنت بحريه كامله وأصبح بإمكان المسافرين في الأول من أبريل **2004** على متن طائرات شركة طيران المانيه خلال الرحلات عبرت المحيط الأطلسي استخدام المحمول للاتصال بالإنترنت وكل هذا بفضل التقنية الجديدة وهي الشبكات المحلية اللاسلكيه **WLAN wireless local area network** وتسمح هذه التقنية بالاتصال بشبكة الإنترنت عبر إشارة الراديو **radio frequency RF** بدلا من الاتصال عبر الأسلاك. اما النقاط الساخنة فهي عباره عن الأماكن التي يستطيع الشخص فيها استخدام تقنية الربط اللاسلكي بالإنترنت. ان عدد النقاط الساخنة وصل إلى مئات الالاف في جميع أنحاء العالم بحلول عام ٢٠٠٥ تعتمد تقنية النقاط الساخنة على عنصرين رئيسيين للاتصال:

1 - بطاقات الحاسب اللاسلكيه (**wireless computer cards**) وقد تكون موجوده بالجهاز المحمول أو أي جهاز آخر أو قد تكون قابلة للاضافه به.تحتوي هذه البطاقه على هوائي داخلي أو خارجي.

2 - نقطة الوصول (**access point**) التي تصل الشبكات المحلية اللاسلكيه بشبكة الإنترنت. اما بالنسبة للطائرات التي تحتوي على نقاط ساخنه فيتم حل مشكلة نقطة الوصول عبر هوائي خارج الطائرة مرتبط باقمار صناعيه خاصه تصله بالشبكة عبر محطات استقبال ارضيه.

استخدامات الشبكات اللاسلكية :

لعبت الشبكات اللاسلكية دوراً كبيراً في الاتصالات العالمية منذ الحرب العالمية الثانية فعن طريق استخدام الشبكات اللاسلكية، يمكن إرسال معلومات لمسافات بعيدة عبر البحار بطريقة سهلة ،عمليّة وموثوقة. منذ ذلك الوقت، تطورت الشبكات اللاسلكية بشكل كبير وأصبح لها استخدامات كثيرة في مجالات واسعة، نذكر منها:

الهواتف الخلوية تشكل أنظمة شبكات ضخمة حول العالم يزداد استخدامها يومياً للتواصل بين أشخاص من جميع أنحاء العالم.

إرسال معلومات كبيرة الحجم لمسافات شاسعة أصبح ممكناً من خلال الشبكات اللاسلكية من خلال استخدام الأقمار الصناعية للتواصل.

الاتصالات العاجلة - كاتصال أفراد الشرطة مع بعضهم - أصبحت أسهل بكثير باستخدام الشبكات اللاسلكية.

أصبح بإمكان الأفراد والشركات على حدّ سواء استخدام هذه الشبكات لتوفير اتصال سريع سواءً كان ذلك على مسافات قريبة أو بعيدة.

من أهم فوائد الشبكات اللاسلكية هو استخدامها كوسيلة رخيصة وسريعة للاتصال بالإنترنت في المناطق التي لا توجد فيها بنية تحتية تسمح بتوفير هذا الاتصال بشكل جيد كما هو الحال في معظم الدول النامية .

إيجابيات وسلبيات استخدام الشبكات اللاسلكية

من أهمها التي جعلتها تنتشر بشكل كبير وتحلّ محل الشبكات السلكية :

المرونة (**wirelessness**) للشبكات اللاسلكيه فوائد أكثر من الشبكات السلكيه وإحدى هذه الفوائد المرونه إذ تمر موجات الراديو بالحيطان والحاسوب اللاسلكي يمكن أنت يكون في أي مكان على نطاق الاكسس بوينت.

سهولة الاستخدام: الشبكات اللاسلكيه سهلة إلى الاعداد والاستعمال فقط برنامج مساعد وتجهيز الحاسوب النقال أو الدسك توب ببطاقة شبكة اصالات لاسلكيه وهناك حواسب مجهزه بهذه البطاقه مثل أجهزة سنترينو.

التخطيط: ان الشبكات السلكيه واللاسلكيه يجب أن تكون مخططه بدقه ولكن الاسوء في الشبكات السلكيه انه يجعل منظر الجدران غير مرتب وتعدد الاجهزة يكلف في عملية الصيانه ان مكونات الشبكات السلكيه هي (كابلات ،سويتش) لذلك يجب أن نخطط لها بعنايه اما بالنسبة للشبكات اللاسلكيه فهي أسهل بكثير من ذلك المنطق ولكن يجب أن نخطط لهذه الشبكات لانماط الاستعمال الفعليه

مكان الاجهزه : الشبكة اللاسلكيه يمكن تكون مخفيه يمكن ان توضع من وراء الشاشات و هذه الشبكات مناسبه تماما للأماكن أو المواقع التي يكون من الصعب ربط شبكه سلكيه فيها مثل المتحف البنايات القديمة.

المتانه: شبكات اللاسلكي ممكن ان تكون متينه ولكن ممكن ان تعاني من التداخل الاذاعي من الأجهزة الآخر والأداء يمكن ان يضعف عند محاولة المستخدمين استعمال نفس الاكسس بوينت.

الأسعار: ان أسعار الشبكات اللاسلكيه كانت غاليه كانت بطاقة الـ **PCI** اللاسلكيه تكلف **100** يورو عام **200** وفي نهاية **2004** أصبحت تكلف **30** يورو فقط وهذا يعني ان الأسعار الآن ليست عاليه وان الشبكات اللاسلكيه أصبحت اختيار الكثير من مستخدمي البيوت.

على الرغم من هذه الفوائد، فإن الشبكات اللاسلكية لا تخلو من بعض المشاكل لعل أهمها:

مشكلات التوافق: فالأجهزة المصنوعة من قبل شركات مختلفة قد لا تتمكن من الاتصال مع بعضها أو قد تحتاج إلى جهد إضافي للتغلب على هذه المشاكل.

إن الشبكات اللاسلكية تكون غالباً أبطأ من الشبكات الموصولة مباشرةً باستخدام تقنيات الإيثرنيت **Ethernet**

الشبكات اللاسلكية أضعف من حيث حماية الخصوصية لأن أي شخص ضمن مجال تغطية شبكة لاسلكية يمكنه محاولة اختراق هذه الشبكة. من أجل حل هذه المشكلة، يوجد عدةبرامج تؤمن حماية للشبكات اللاسلكية مثل الخصوصية المكافئة للشبكات السلكية **Wired Equivalent Privact WAP** التي لم تؤمن الحماية الكافية للشبكات اللاسلكية والـ **Wi Fi Protected Access WPA** التي أظهرت نجاحاً أكبر في منع الاختراقات من سابقتها.

مخاوف صحية من الشبكات اللاسلكية :

في الآونة الأخيرة، ازدادت المخاوف من مخاطر الشبكات اللاسلكية والحقول الكهرومغناطيسية التي تولّدها على الرغم من عدم وجود أدلة قاطعة تثبت صحة هذه الإداعاءات فعلى سبيل المثال، رفض رئيس جامعة **Lakehead** في كنداإنشاء شبكة لاسلكية ضمن حرم الجامعة بسبب دراسة تقول أن تأثير التعرض للحقول الكهرومغناطيسية الناتجة عن الشبكات اللاسلكية على الإصابة بسرطانات وأورام يجب أن يُدرس بشكل أكبر قبل تحديد مدى هذا التأثير.

البروتوكول IEEE 802.11 :

البنية الطبقية للمعمارية **IEEE 802.11**

الطبقة الفيزيائية : هي طبقة مجسمة تتألف من مجموعة من المكونات الفيزيائية وهي تعتمد عادة على إحدى التقنيات الثلاث التالية:

الأشعة تحت الحمراء **Infrared IR**

الطيف متغير الترددات **Frequency Hopping Spread Spectrum FHSS**

الطيف ذو التردد المباشر **Direct Sequence Spread Spectrum DSSS**

كما تؤسس على هذه الطبقة باقي طبقات البروتوكول والتي تكون مسؤولة عن عملية التخاطب لإنجاز نقل البيانات.

طبقة :MAC طبقة مراقبة الوصول الإعلامي. تعرف هذه الطبقة طريقتين مختلفتين للوصول : وظيفة التنسيق الموزع **Distributed Coordination Function** ووظيفة التنسيق النقطي **Point Coordination Function** ملاحظة إن الـ **MAC Layer** تتوضع عند قمة الطبقة الفيزيائية، وبدوره عامل التنسيق الموجه يتوضع على قمة عامل التنسيق الموزع.

نهاية الكتاب

مما سبق يتبين أن هذا الموضوع من الأهمية بمكان وينبغى أن تتوجه إليه الجهود ويحظى بالعناية والاهتمام وينبغى أخذ الدروس والعبر التى تفيد الفرد والمجتمع وبهذا أكون قد انتهيت من كتابة هذا الكتاب وأسال الله أن أكون قد وفقت فيه .

مراجع الكتاب :

CCNA Routing and Switching ICND2 200-101 Official Cert Guide By Wendell Odom

CCENTCCNA ICND1 100-101 Official Cert Guide By Wendell Odom

Cisco CCNA Routing and Switching (200-120) Official Cert Guide Library

Cisco CCNA Routing and Switching How to Master

وسلام عليكم و رحمة الله و بركاته